candide
media works

Projet Sécurité des SI

Groupe Défense :

candide
media works

Auteurs :

Georges-Henri **Epacka**
Nicolas **Lin Wee Kuan**
David **Richet**
Boris **Longevialle**
Cédric **Pauthe**
Daniel **Valsadia**
Romain **Bottan**
Julien **Moutet**
Jérôme **Pottier**

Année Universitaire 2005-2006 :

Université Toulouse III - Paul Sabatier
IUP – MASTER STRI (Systèmes de Télécommunications et Réseaux Informatiques)

SOMMAIRE

1 PRESENTATION ____ 3

1.1 Projet Sécurisation des SI ____ 3

1.2 De l'équipe Défense ____ 4

1.2.1 Direction du Système d'Information (DSI) ____ 4
1.2.2 Coordination ____ 5
1.2.3 Service Technique ____ 5

1.3 Analyse de l'existant ____ 5

1.4 Planning ____ 6

2 ANALYSE DES BESOINS ____ 9

2.1 Utilisateurs ____ 9

2.1.1 Poste de travail ____ 9
2.1.2 Services souhaités ____ 10

2.2 Réseau ____ 10

2.2.1 Structure ____ 10
2.2.2 Tolérance de panne ____ 11
2.2.3 Performance ____ 11
2.2.4 Facilité de déploiement ____ 11
2.2.5 Sécurité ____ 11

3 ETUDE PRELIMINAIRE AU CAHIER DES CHARGES ____ 13

3.1 Services offerts ____ 13

3.1.1 Utilisateurs internes ____ 13
3.1.2 Utilisateurs externes ____ 14

3.2 Réseau / Architecture ____ 14

3.2.1 Contraintes physiques ____ 14
3.2.2 Présentation de l'architecture choisie ____ 14
3.2.3 Recensement du matériel ____ 16

3.3 Politique de sécurité ____ 19

3.3.1 Description de la phase 1 ____ 19
3.3.2 Description de la phase 2 ____ 23

4 ETUDE DETAILLEE DU CAHIER DES CHARGES ____ 29

4.1 Association Service – Matériel ____ 29

4.2 Etude de la sécurité ____ 31

4.2.1 Mise en place effective de la phase 1 ____ 31
4.2.2 Mise en place effective de la phase 2 ____ 33

5 RETOUR SUR INVESTISSEMENTS ____ 36

5.1 Etude des risques ____ 36

5.2 Communication ____ 36

5.3 Gestion des incidents ____ 37

6 Conclusion ____ 39

1 PRESENTATION

1.1 Projet Sécurisation des SI

Le projet de sécurisation des systèmes d'informations proposé lors de cette dernière année du Master STRI a pour objectif de nous faire découvrir l'importance des processus de sécurité à partir de cas concrets et pratiques mettant en scène plusieurs acteurs fictifs représentant la réalité de l'entreprise dans ses moindres détails. Ces acteurs ont été définis au préalable en trois groupes bien distincts :

- Groupe Défense : il met en place un système d'information ainsi que les services appropriés. Il doit mettre en place une politique de sécurité de différents niveaux.

- Groupe Analyse : il collecte un maximum d'informations et de données sur le SI pour les analyser et identifier les actions entreprises aussi bien par le groupe de défense que celui d'attaque.

- Groupe Attaque : il se charge de rechercher toutes les possibilités d'intrusions et/ou de compromissions possible sur le SI. Il s'agit pour ce groupe de mettre en œuvre par tous les moyens à leur disposition une attaque du SI.

Pour ses trois groupes, une gestion et une organisation a été mise en place. Chaque groupe dispose d'une liste de diffusion à laquelle est attachée un espace documentaire privatif. Ces listes sont l'outil principal de communication et surtout de coordination du groupe.

1.2 De l'équipe Défense

Le travail de l'équipe Défense consiste à simuler une entreprise nommée Candide SA afin d'aborder les différents aspects de la sécurité du système d'information d'une société et d'appréhender les différents phases de la gestion de projet. De ce fait, pour permettre à toutes les équipes de ce projet de profiter au mieux d'une telle expérience en matière de découverte d'un SI, nous avons choisi de découper notre action en deux temps.

Tout d'abord, l'équipe de défense mettra en place un SI basé sur des niveaux de sécurité faibles. Dans cette première phase, que nous appellerons « phase n°1 », nous pourrons observer l'effet néfaste des pirates sur une architecture peu protégée, ainsi, nous réagirons en fonction de l'efficacité de leurs attaques et notre politique de réaction.

Dans un deuxième temps, nous utiliserons nos connaissances en matière de sécurité pour, à juste titre, sécuriser au maximum la structure d'informations qui a été mise en place. Nous tenterons ensuite d'évaluer les risques ainsi que les failles de notre système d'informations. Il s'agira alors de la « phase n°2 ».

Pour une organisation optimale au sein du groupe Défense, on a décidé de nous subdiviser en sous-groupe afin d'améliorer la performance du groupe Défense. Trois groupes ont alors été définis :

- Direction du Système d'Information (DSI).
- Coordination.
- Service technique.

1.2.1 Direction du Système d'Information (DSI)

La direction du système d'information est responsable de la stratégie informatique de l'entreprise. La DSI n'a pas seulement besoin de connaissances en informatique. Elle doit aussi organiser et manager la mise en place du SI au sein de l'entreprise. La DSI a pour missions principales d'assurer :

- la conception, l'élaboration et le suivi du schéma directeur du système d'information,
- l'évolution du système d'information à partir de l'expression des besoins des utilisateurs, dans une démarche planifiée,
- la réalisation du SDSI par la conduite des projets d'informatisation en veillant à la cohérence fonctionnelle et technique, à la qualité

et à la sécurité du système d'information et à la maîtrise des coûts et des délais,

- la définition, du choix et de la mise en œuvre des méthodes, normes et standards informatiques

1.2.2 Coordination

Ce sous-groupe a en charge la communication interne et externe sur le projet. Il s'agit pour lui de rassembler, organiser, interpréter et présenter des rapports d'informations aussi bien en interne (vis-à-vis des autres sous-groupes de l'équipe Défense) qu'en externe (vis-à-vis d'un éventuel prestataire externe ; ici le groupe Analyse du projet) tout en gardant une éthique propre à l'entreprise.

Le groupe coordination joue ainsi le lien de médiateur interne et externe et doit notamment gérer un planning d'activités pour synchroniser les diverses actions qui pourraient être menées ensemble.

1.2.3 Service Technique

Le service technique assure la maîtrise d'œuvre relative à la gestion des infrastructures et au support du Système d'Information. Ses missions sont réalisées dans un objectif de qualité et de productivité, au service des utilisateurs, tant dans la gestion de leurs demandes que dans la disponibilité des applications qu'ils utilisent. A ce titre, elle doit effectuer la gestion de proximité nécessaire à la bonne mise en œuvre et utilisation des équipements informatiques.

En d'autres termes, le service technique administre le support et la définition de l'environnement utilisateur ainsi que les équipements informatiques de la société.

Ce service effectue des tâches comme :

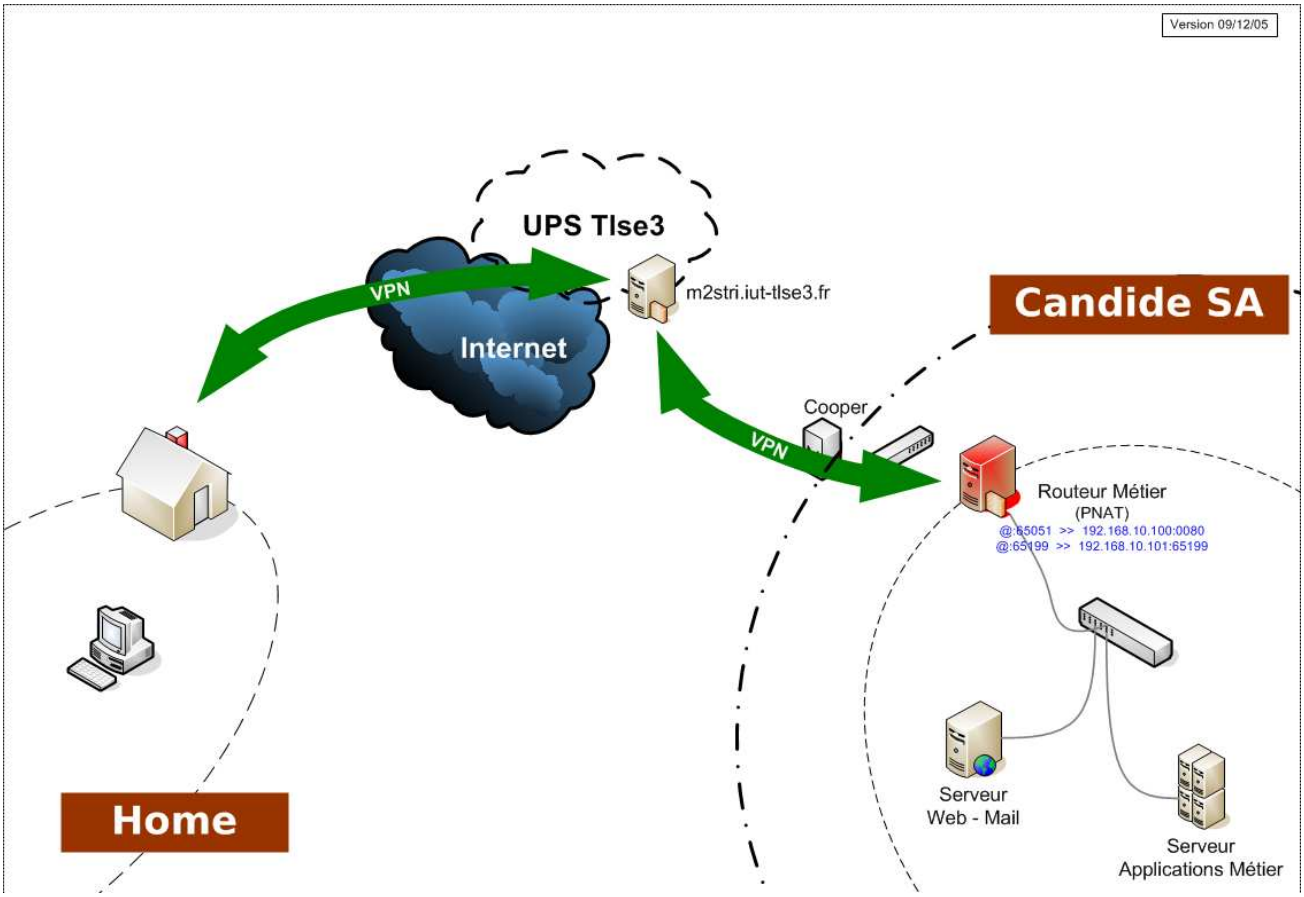
- Installation et réparation des équipements, systèmes, etc.
- Configuration fichier / serveur / système.
- Simulation du réseau / d'un utilisateur du réseau.
- Lister les paramètres configurables sur les équipements tels que les routeurs et autre.

1.3 Analyse de l'existant

Pour mettre en place l'architecture réseau de la société Candide, nous disposons d'équipements d'interconnexion réseau : des commutateurs et des concentrateurs, ainsi que six machines vierges.

Notre architecture, pour des raisons de sécurité est mise en place à l'intérieur même du réseau de l'université et n'est accessible de l'extérieur uniquement grâce à un point de contact qui est la machine « m2.stri-iut.tlse3.fr ». Elle permet de passer au travers du routeur GNU/Linux Cooper qui filtre le trafic.

L'accès à nos machines se fait grâce à des tunnels (VPN) jusqu'à Cooper qui lui-même redirigera les flux vers le réseau de Candide SA.



En utilisant ce tunnel, nous pourrons administrer nos serveurs ainsi que nos clients.

1.4 Planning

Pour la gestion de l'équipe, nous avons employé du mieux que possible la gestion de charges et du temps de travail. Cette volonté de gérer les différentes sous équipes de manière temporelle et axée charge de travail nous a accompagné durant toute la durée du projet.

Etape initiale :

Le partage de l'équipe Défense en 3 sous-groupes pour nous répartir la charge de travail :

- Equipe Technique : Recenser le matériel,
- Equipe Coordination : Planifier et gérer la communication interne,
- Equipe DSI : Commencer à étudier l'architecture

Mise en place de l'architecture :

- Les plus de cette étape :

  + L'équipe DSI s'est substituée en supplément à l'équipe Technique pour mettre en place la solution de la DSI,
  + L'équipe Coordination a commencé à rédiger le rapport final à l'aide des spécifications DSI et des rapports Techniques et organisé des réunions Défense avec leur bilan.

- Les moins de cette étape :

  - Sous estimer les temps de mise en place de l'architecture
  - L'équipe DSI a voulut mettre des règles de sécurité trop forte

Exploitation de l'architecture :

- Les plus de cette étape :

  + L'équipe DSI observe les journaux, réagit, trouve les parades aux attaques,
  + L'équipe Technique joue le rôle des clients,
  + L'équipe Coordination s'occupe du rapport,

- Les moins de cette étape :

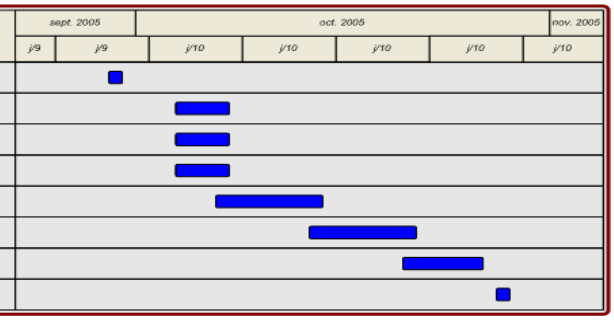
  - Attente des attaquants

Aide au rapport :

+ Les équipes DSI et Technique sont associées à chacun des membres de l'équipe Coordination afin de permettre une élaboration plus rapide du rapport,
+ L'équipe DSI travaille en parallèle sur l'exploitation.

Planning prévisionnel :

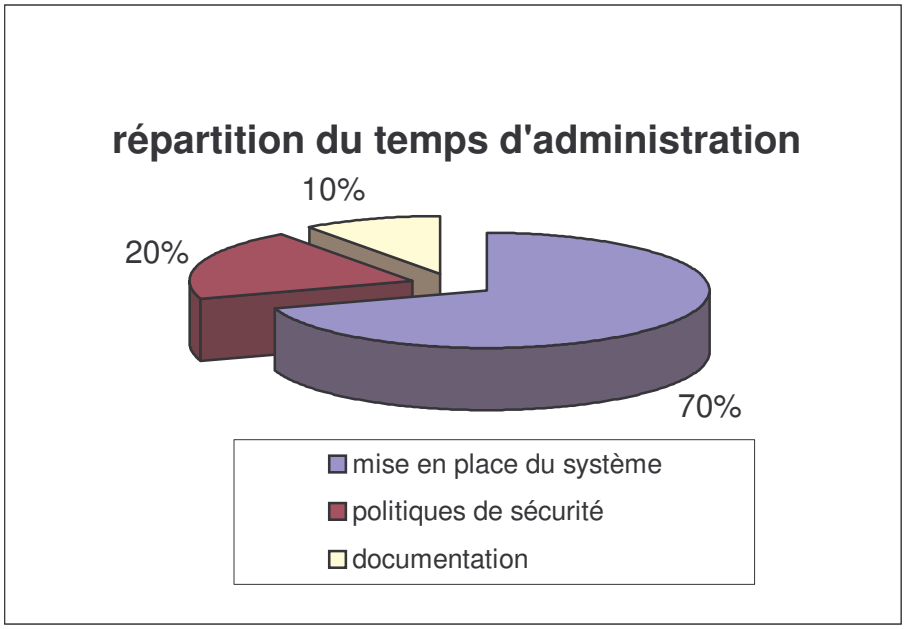
ID	Nom de tâche	Début	Terminer	Durée
1	Définition des rôles	29/09/2005	29/09/2005	1j
2	Audit – Planning - Architecture de départ	04/10/2005	07/10/2005	4j
3	Mise en place du réseau	04/10/2005	07/10/2005	4j
4	Audit des flux	04/10/2005	07/10/2005	4j
5	Etudes des services à mettre en place	07/10/2005	14/10/2005	6j
6	Création de la sécurité	14/10/2005	21/10/2005	6j
7	Réalisations, Mise en place de la sécurité	21/10/2005	26/10/2005	4j
8	Audit des flux	28/10/2005	28/10/2005	1j



Ce planning n'a pas pu être tenu à cause de certains problèmes rencontrés pendant ce projet, notons :

- le manque de temps,
- le manque d'investissements de certains,
- la surestimation des capacités de l'équipe d'Attaque qui a engendré une politique de sécurité de phase 1 trop élevé et donc plus difficile à mettre en place,
- les problèmes de matériels qui ont fait perdre un temps monstrueux.

Pour simplifier, nous nous retrouvons dans une répartition du temps comme suit :



Alors que nous aurions dû passer la majeure partie de notre temps sur l'élaboration de la politique de sécurité.

2 ANALYSE DES BESOINS

Avant de mettre une architecture en place, il faut se poser des questions qui permettront de dimensionner la solution réseau. Ces dimensions prendront en compte :

- le nombre de postes clients,
- les applications nécessaires,
- les besoins en accès des utilisateurs du réseau,
- le niveau de sécurité souhaité, etc.

Nous ne perdons pas de vue que le but de ce projet soit, d'établir une solution la plus proche de celle d'une entreprise afin que l'implémentation de cette dernière soit la plus proche d'un cas concret.

Contraintes physiques :
- de performance réseau,
- du nombre de postes mise à disposition,
- de performance des postes.

Analyse des besoins en terme :
- clients : facilité d'utilisation, outil simple à manipuler,
- application : serveur métier où tourne des applications métier,
- communications : serveur Web, serveur Mail,
- sécurité : doit permettre une évolution facile.

A partir de ces contraintes et de nos besoins, la solution peut se dessiner petit à petit. De plus, à partir de statistiques trouvées sur journaldunet.com, nous avons pu avoir une idée de ce qu'il se faisait majoritairement dans les petites et moyennes entreprises.

Pour mieux tester les différentes politiques de sécurité choisies en PME, nous avons décidé d'implémenter une architecture classique et simple permettant une mise en place de niveau de sécurité implémenté dans une petite structure.

Vous l'avez bien compris, l'architecture et la politique de sécurité sont un compromis entre les besoins des utilisateurs, les besoins des administrateurs, le célèbre DIC (Disponibilité, Intégrité, Confidentialité), la performance et la facilité de déploiement.

2.1 Utilisateurs

2.1.1 Poste de travail

Les postes de travail des utilisateurs doivent être facilement manipulable pour toutes personnes. Pour cela, en accord avec les statistiques trouvées

sur le choix du système d'exploitation des clients, nous avons choisi d'installer *Microsoft Windows XP*.
Sera installé et configuré sur les postes clients les outils nécessaires à leur travail :

- un client mail,
- un navigateur Internet,
- et un éditeur de texte.

Ces outils sont bien souvent intégrés dans les systèmes d'exploitation de Microsoft, ce qui nous permettra une configuration cliente beaucoup plus rapide.

2.1.2 Services souhaités

Pour correspondre au minimum au fonctionnement d'une entreprise, nous avons choisi d'implémenter différents services :

- Mail : Ce service permettra aux utilisateurs d'avoir une adresse mail à l'effigie de l'entreprise pour pouvoir communiquer de manière plus professionnelle,

- DNS : Ce protocole assure la correspondance entre le nom d'une machine et son adresse IP,

- DHCP : Ce protocole est utilisé pour délivrer dynamiquement une adresse IP unique pour chaque machine le demandant sur le réseau interne. Ce service permet d'alléger la gestion du réseau en évitant d'avoir des configurations statiques à maintenir sur chaque machine.

- Web : serveur de présentation à l'Internet de Candide SA

2.2 Réseau

2.2.1 Structure

Notre architecture est celle qui est utilisée normalement dans toute infrastructure de PME. Une séparation physique entre le parc métier et le parc informatique est donc appliquée dans notre architecture.

Le réseau de Candide SA dispose d'un routeur de tête de type Cisco 3620. Sous ce routeur, schématiquement, se trouvent 2 passerelles qui définissent l'entrée des sous réseaux suivants :

- Sous réseau Métier,
- Sous réseau Parc.

Dans le sous réseau métier se trouve les serveurs de l'entreprise, les serveurs de présentation et de communication ainsi que les serveurs d'application métier.

2.2.2 Tolérance de panne

La tolérance de panne dans un système d'information est souvent la question la plus délicate. Elle peut se faire dans deux niveaux, système et réseau.

Dans notre cas, un manque de machine nous empêchera de redonder nos équipements et nous ne pourrons donc faire de redondance système/services. Dans un souci de continuité de service, un seul service permettant aux utilisateurs de travailler en cas de panne d'un des routeurs, sera redondés, il s'agit du serveur DNS qui devra être présent sur les deux routeurs de tête.

Notre choix d'infrastructure a été basé sur la tolérance de panne. Si le routeur de la branche métier défaille, les utilisateurs pourront quand même accéder à Internet, mais ils ne pourront plus se servir de leur mail. Si le routeur du parc informatique défaille, les serveurs de présentation seront toujours disponibles.

2.2.3 Performance

Notre architecture est pensée pour avoir une meilleure performance, car chaque requête ne traverse qu'un seul routeur et qu'une seule règle de sécurité, ce qui implique que notre réseau fonctionne plus vite et qu'il est moins surchargé.

2.2.4 Facilité de déploiement

L'avantage d'avoir deux sous réseaux distincts est de pouvoir contrôler et gérer la mise en place des services. Cette structure de réseau regroupé permet un déploiement plus efficace. Ce qui en cas de panne facilite le re-déploiement. La sécurisation de notre réseau est centralisée.

2.2.5 Sécurité

Il y a deux méthodes de sécurisation :

- Sécurisation des postes clients : réseau transparent, clients lourds.
- Sécurisation réseau : postes clients léger non protégé, performance réseau atténuée.

Chacune de ses techniques présente des avantages. De nos jours, nous utilisons ces deux techniques ; donc pour notre réseau nous avons appliqué cette politique.

La solution de sécurité de penser de manière à pouvoir évoluer rapidement. Cette pensée nous permettra donc de se rapprocher du modèle réel, et de pouvoir déployer la phase 2 plus rapidement.

Le réseau doit fournir une sécurisation des niveaux 3 et 4 du modèle OSI. Pour cela, nous nous chargerons les pare-feux de Debian : NetFilter. Cet outil nous permettra de configurer le niveau de sécurité voulu. Les détails sécurité des serveurs, des systèmes, des routeurs, des différentes phases seront traités dans les parties suivantes.

Contrairement à l'idée reçue, une politique de sécurité n'est pas un luxe réservé aux grandes entreprises. Les PME aussi en bénéficient, à condition de savoir rédiger - et de faire accepter par tous les collaborateurs - ce document de référence.

Son objectif : décrire les mesures élémentaires de protection et d'utilisation du système d'information de l'entreprise, afin que tout le monde puisse les respecter.

Par exemple, "l'utilisation acceptable des outils informatiques" ou "la charte d'utilisation destiné aux utilisateurs" détaille ce que l'employé aurait le droit de faire et de ne pas faire avec son poste de travail. Elle couvre des sujets tels que les mails personnels, le téléchargement d'images ou de fichiers multimédia, l'installation de logiciels personnels sur le poste, la propriété de l'information qui y est manipulée, etc. C'est aussi l'occasion de rappeler le contexte légal de l'utilisation de l'outil informatique (droits d'auteurs, stockage de matériel pornographique, interdiction du piratage, du Spam, du harcèlement par mail, etc.).

La définition des politiques de sécurité sera définie de la façon suivante :

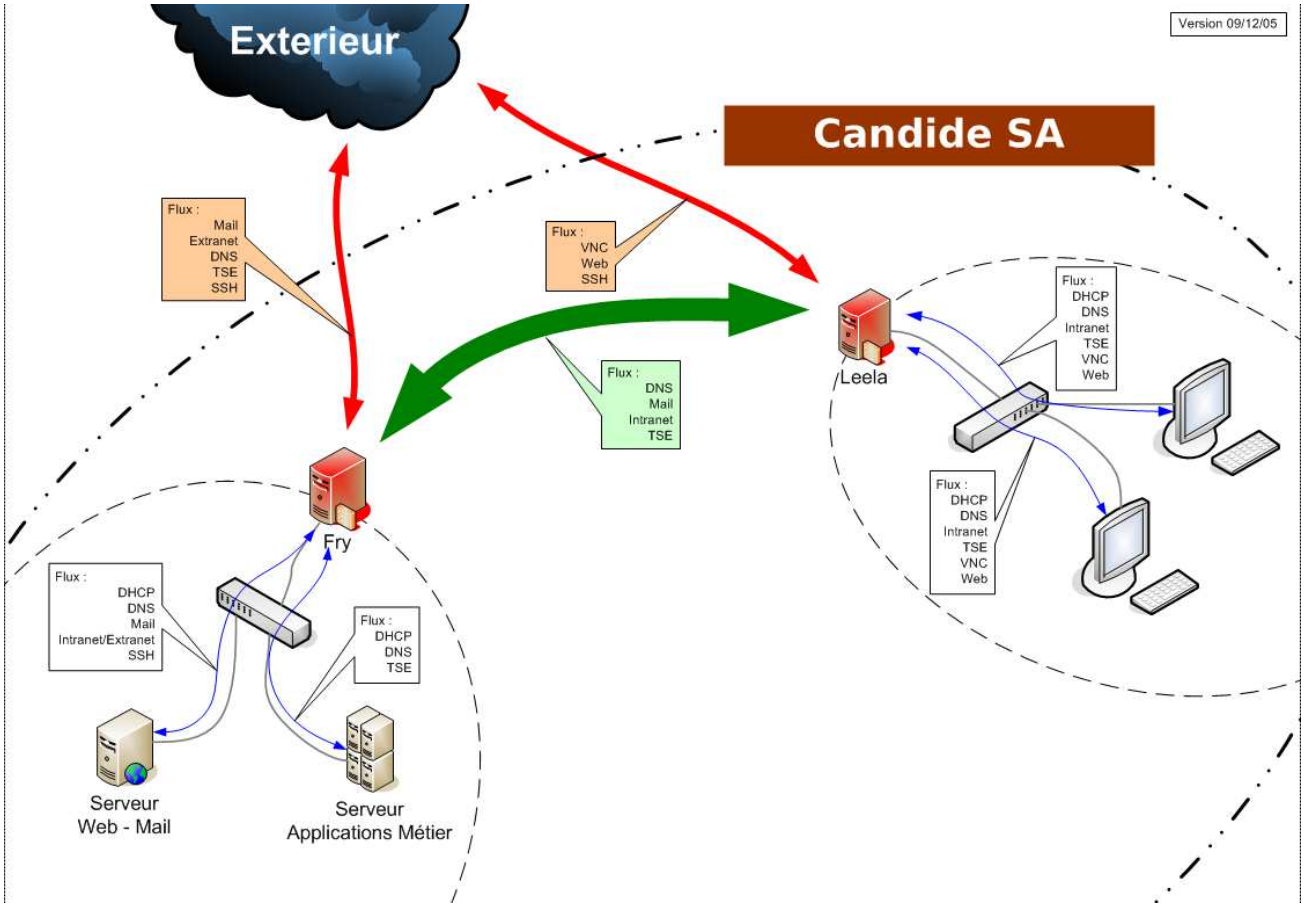
- Politique d'utilisation acceptable du réseau
- Politique de Mail
- Politique de mot de passe
- Politique de sécurité du routeur et des équipements
- Politique de sécurité des serveurs et des pare-feux.

3 ETUDE PRELIMINAIRE AU CAHIER DES CHARGES

3.1 Services offerts

Après consultation des besoins évalués par l'équipe DSI, nous décidons de mettre en place un certain nombre de services, correspondants aux flux qui doivent transiter sur notre réseau.

Le schéma ci-dessous décrit les flux entrants et sortants de Candide S.A. :



Les services de résolution de noms (DNS) et de résolution d'adresses (DHCP) sont implémentés sur les routeurs du réseau. Ils sont transparents de configuration pour les utilisateurs et ne seront donc pas évoqués dans cet inventaire.

3.1.1 Utilisateurs internes

Les utilisateurs internes au réseau local de Candide S.A. sont les employés disposant d'un poste informatique de travail. Leur accès au réseau respecte la politique de sécurité de l'entreprise définie par « *Acceptable Use Policy* » définit dans les parties suivantes du rapport.

Ils ont accès à Internet (service http) via leurs postes de travail, de plus, Candide SA offre un service mail (pop et smtp).

Ils ont accès au serveur d'applications où s'exécutent leurs applications Métier utilisant l'intranet et des bases de données.

Via le mode TSE (Terminal Server Edition), ils peuvent exécuter des applications lourdes permettant d'alléger un client. Ceci simplifie le déploiement logiciel des machines clientes, qui ne nécessitent donc pas une puissance de calcul processeur trop importante.

3.1.2 Utilisateurs externes

Par utilisateur externe, nous entendons toute personne, non salariée de l'entreprise, souhaitant utiliser les services offerts par Candide SA. En l'occurrence, il s'agit ici du service web correspondant au site Internet de l'entreprise.

Pour simplifier les administrateurs, nous ouvrirons un service SSH sur les routeurs, ceci permettra une entière manipulation des routeurs.

3.2 Réseau / Architecture

3.2.1 Contraintes physiques

Nous avons dû simuler le réseau de l'entreprise avec un nombre de micro-ordinateurs limité à six, ne permettant bien évidemment pas d'être dans un contexte réel.

Nous avons donc déclaré des machines clientes représentatives et restreint l'utilisation des serveurs. Aucune, dans cette configuration machine n'est redondante.

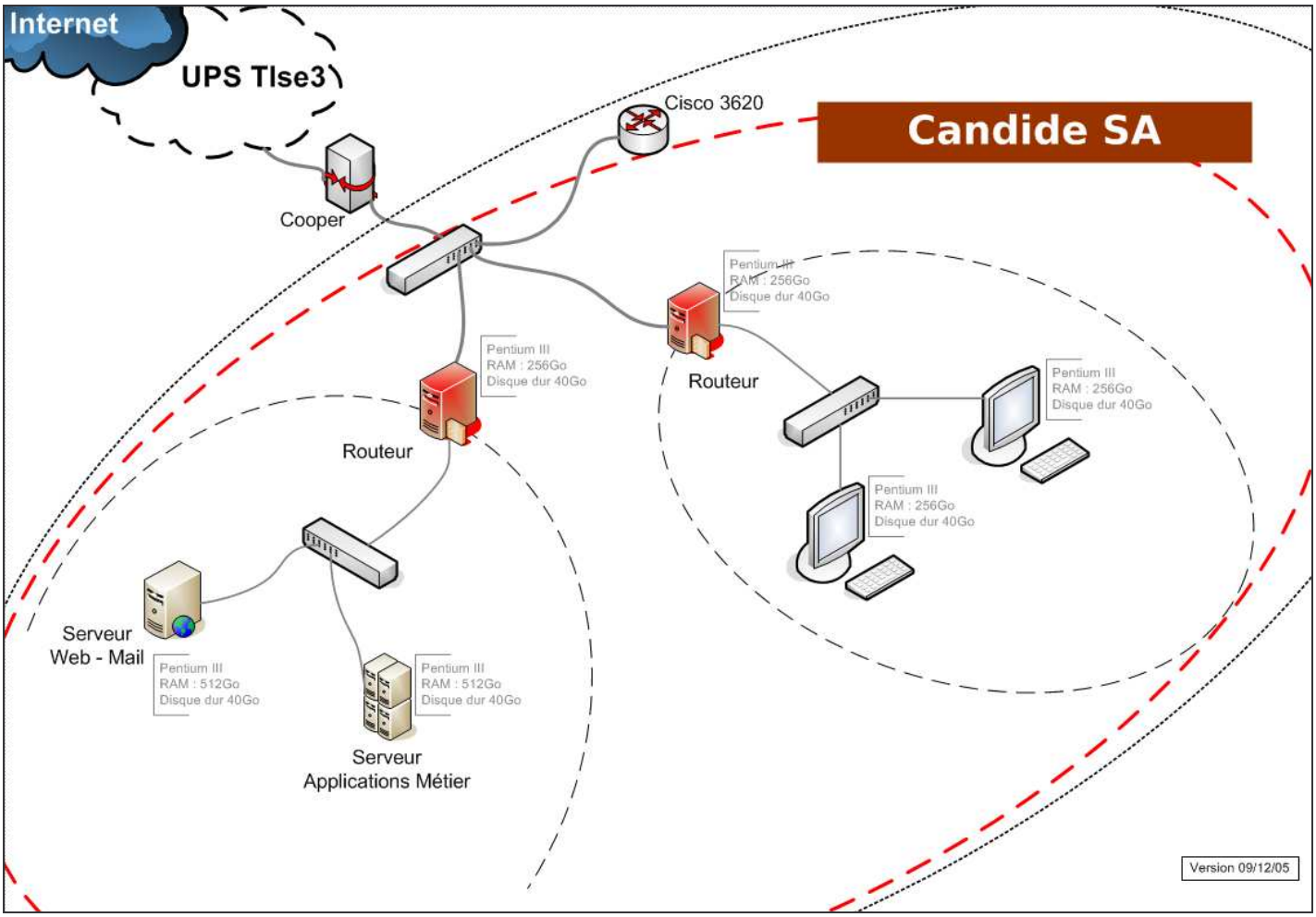
De plus, ces micro-ordinateurs n'ont pas des configurations leur permettant de jouer réellement les rôles de serveurs et passerelles qui disposent d'alimentations redondantes ainsi que des disques durs en RAID, ce qui n'offre aucune tolérance aux pannes au niveau système d'information.

Nous avons ainsi rencontré des problèmes sur ces points car un boîtier d'alimentation, les cartes réseau et un disque dur étaient défectueux, paralysant le fonctionnement du réseau et retardant le projet dans son ensemble.

3.2.2 Présentation de l'architecture choisie

Notre architecture est celle qui est normalement utilisée dans toute infrastructure d'une PME.

Physiquement, nous obtenons l'architecture suivante :



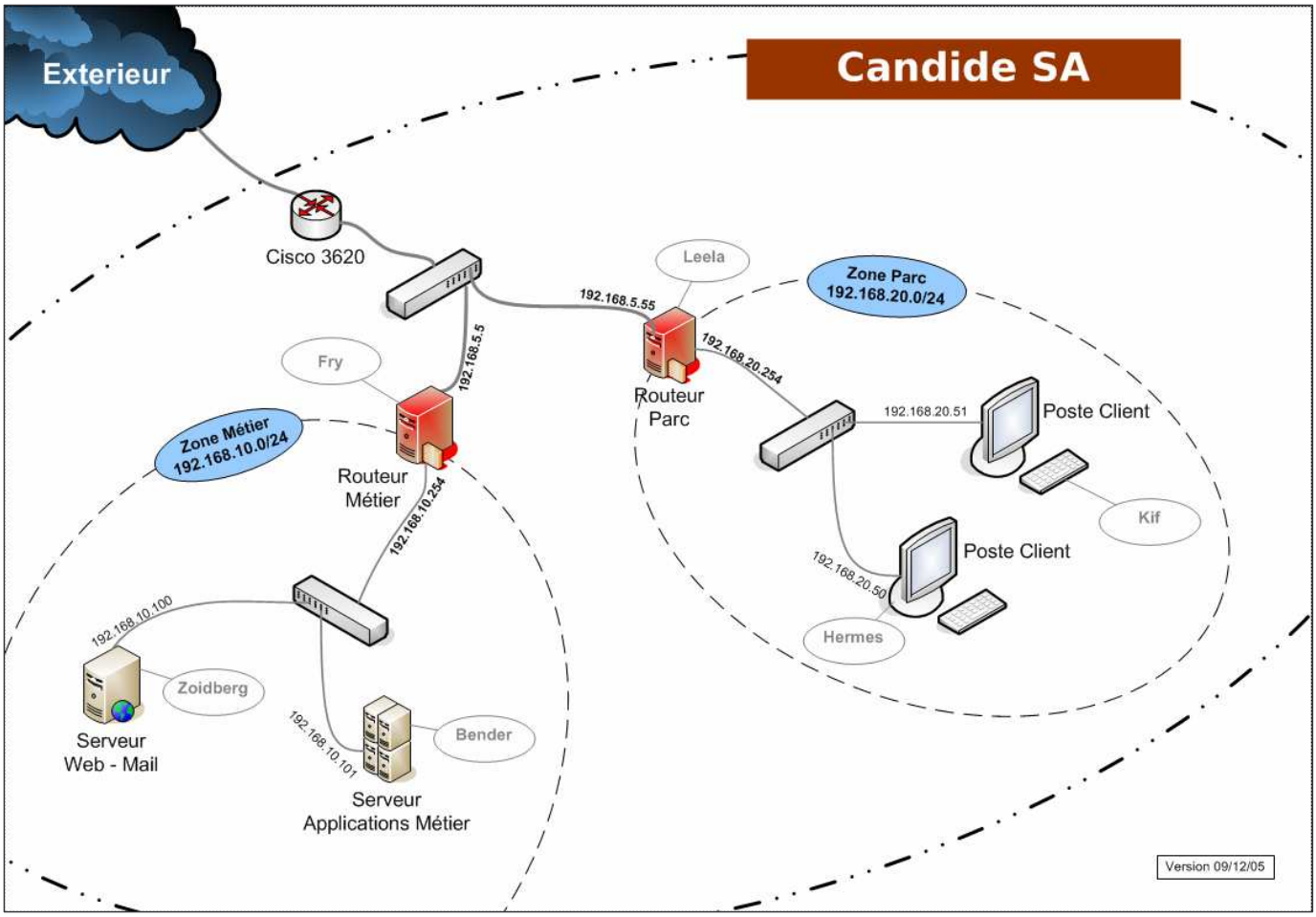
Cette architecture répond à toutes les exigences en terme de performances et de sécurité puisque les serveurs et les postes clients sont physiquement séparés. Elle est aussi évolutive.

Le plan d'adressage de la Candide SA est relativement simple. Les adresses IP externes sont du type 192.168.5.0/24 données par M. Latu.

Nos routeurs effectuant du NAT, servent les réseaux :

- 192.168.10.0/24
- 192.168.20.0/24

Les machines dans les sous réseaux ont une adresse qui correspond à la plage IP distribuée. Toutes nos machines ont un nom simple, pour pouvoir les identifier plus facilement.



3.2.3 Recensement du matériel

Le tableau suivant recense le matériel, les services, les applications et le rôle de chaque machine :

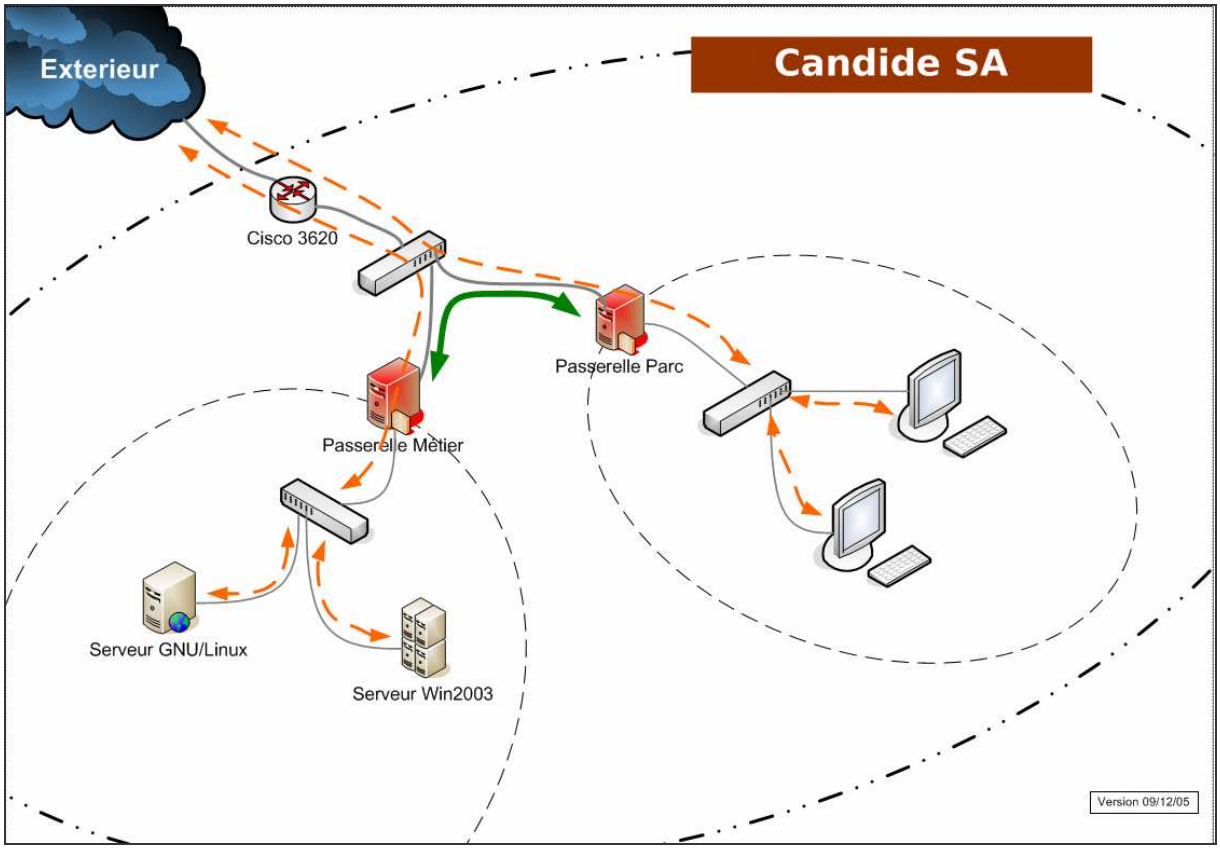
Domaine	Candide SA					
Nom Machine	Fry	Leela	Bender	Zoidberg	Hermes	Kif
Type	Routeur	Routeur	Serveur	Serveur	Poste client	Poste client
Etat	(En Marche)	(En Marche)	(En Marche)	(En Marche)	(En Marche)	(En Marche)
OS	GNU/Linux Debian Sarge	GNU/Linux Debian Sarge	Windows 2003 Server	GNU/Linux Debian Sarge	Windows XP Pro	Windows XP Pro
IP locale (1)	192.168.5.5	192.168.5.55				
IP locale (2)	192.168.10.254	192.168.20.254	192.168.10.101	192.168.10.100	192.168.20.50	192.168.20.51
Matériel						
UC	PC	PC	PC	PC	PC	PC
Carte Mère						
Processeur (MHz)						
RAM (Mo)	(128 Mo)	(128 Mo)	(128 Mo)	(128 Mo)	(128 Mo)	(128 Mo)
Carte Vidéo	(GeForce 4 - 128Mo)	(GeForce 4 - 128Mo)	(GeForce 4 - 128Mo)	(GeForce 4 - 128Mo)	(GeForce 4 - 128Mo)	(GeForce 4 - 128Mo)
Ecran	(CRT 14'')	(CRT 14'')	(CRT 14'')	(CRT 14'')	(CRT 14'')	(CRT 14'')
Lecteur CD	(32X)	(32X)	(32X)	(32X)	(32X)	(32X)
Disque dur (Go)	(8 Go)	(8 Go)	(8 Go)	(8 Go)	(8 Go)	(8 Go)
Serveurs						
HTTP (Apache2)				x		
HTTPS (Apache 2)				x		
IIS			x			
MySQL				x		
MS SQL Server			x			
PHP4				x		
DHCP	X	x				
DNS	X	x				
ACTIVE DIRECTORY			x			
VNC						
Terminal Server			x			
SSH	X	x		x		

Postfix				x		
Stunnel	X	x				
Applications						
MS - Service Pack 1					x	
MS - Service Pack 2					x	
Fix - Blaster / Sasser					x	X
AntiVirus - ClamWin					x	
Microsoft Office 2003			x			
Adobe Acrobat Reader			x			
ACTIVE DIRECTORY			x			
VNC					x	X
MS CLIENT RDP					x	X
SSH	x	x		x	x	X
OpenOffice					x	X
Mozilla-Firefox			x		x	X
Mozilla-Thunderbird			x			

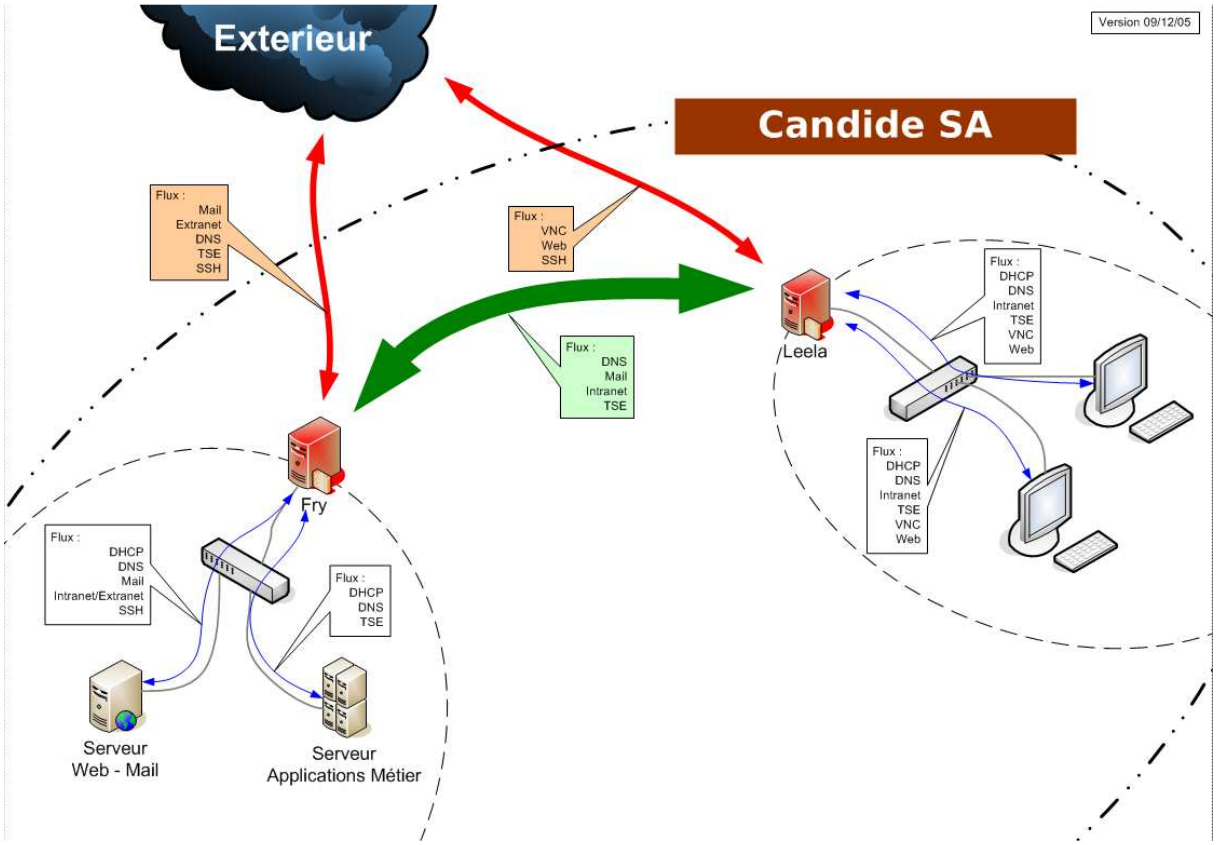
3.3 Politique de sécurité

3.3.1 Description de la phase 1

Les flux globaux transitant peuvent être représenté comme suit :



Plus précisément, nous obtenons :



Le niveau de sécurité de notre réseau est au plus bas et correspond malheureusement à certaines petites structures qui négligent la sécurité de leur réseau.

→ Acceptable Use Policy

Le système d'exploitation des postes clients a été choisi en fonction de la réalité professionnelle dans la majeure partie des grandes sociétés. Nous avons opté pour :

- un poste Client Windows XP Pro
- un poste Client Windows XP Pro SP2

Les utilisateurs ont accès à Internet via leurs postes de travail. Ils sont libres de faire ce qu'ils veulent sur Internet, à leur entière responsabilité.

Ils sont seuls maîtres de leur sécurité et responsable de leur niveau de sécurité au niveau de leur poste de travail. Ils peuvent, s'ils pensent que cela est nécessaire, installer un antivirus et/ou un pare-feu qu'ils paramétreront eux-mêmes.

En résumé, les utilisateurs peuvent installer tous les logiciels à leur convenance sur leur poste de travail, à leur entière responsabilité, à condition évidemment de respecter les lois en terme de propriété intellectuelle.

→ Email Policy

Les utilisateurs doivent obligatoirement utiliser leur compte mail au sein de l'entreprise. Ils ne peuvent toutefois pas consulter ce compte depuis l'extérieur. Libre à eux d'installer des applications clientes pour récupérer leurs mails sur leur poste client.

→ Password Policy

Il faut savoir que les mots de passe utilisés sur un système d'information sont chiffrés pour garantir leur confidentialité. Ces mots de passe chiffrés sont stockés dans des listes de mots de passe sur des fichiers systèmes prédéfinis. Un pirate peut fort bien récupérer ces listes et tester la fiabilité des mots de passe. Il utilise pour cela l'outil adéquat : un perceur de mot de passe.

La plupart des algorithmes de chiffrage repose sur l'utilisation de fonctions à sens unique. Ceci veut simplement dire qu'il est impossible de décrypter le mot de passe à partir de sa forme chiffrée. L'attaque consiste alors à chiffrer différentes combinaisons de caractères et de comparer cette forme chiffrée à celle du mot de passe voulu. Si les deux chaînes correspondent, alors la suite de caractères est celle du mot de passe.

Il y a deux types d'attaques pour le craquage de mots de passe :

- L'attaque par dictionnaire
- Le brute forcing

L'attaque par dictionnaire :
Le programme utilise une liste de mots prédéfinis dans un fichier externe. Cette liste est appelée un dictionnaire ; ces mots sont la plupart du temps ceux provenant d'un dictionnaire contenant les mots du langage courant. Le programme les chiffre avec l'algorithme de chiffrage adéquat un par un et les compare au mot de passe chiffré. Ce type d'attaque est très rapide. Un mot de passe mal choisi est vite découvert.

Le brute forcing :
Si l'attaque par dictionnaire ne marche pas, le programme peut générer des mots de passe avec une suite aléatoire de caractères, les chiffrer et les comparer au mot de passe à découvrir. Avec un mot de passe suffisamment long (supérieur à 8 caractères), cette méthode a peu de chance d'aboutir. Si, de plus, des caractères spéciaux sont ajoutés comme des signes de ponctuation, la méthode peut se révéler inefficace. Il existe différents logiciels de perçage de mots de passe en fonction du type de chiffrage (DES, MD5, spécialement pour Microsoft).

Nous protégerons donc par mot de passe :

- les comptes administrateur sous Windows et sous Debian

- les comptes mail

Les mots de passe seront choisis par les administrateurs systèmes et réseaux. Les utilisateurs ne pourront pas changer de mot de passe et ne doivent en aucun cas communiquer leur mot de passe, que ce soit à leurs supérieurs hiérarchiques ou même à leurs collaborateurs.

Règles :

- Utilisez un mot de passe contenant des lettres en majuscules ET en minuscules. Pas seulement au début de chaque mot, mais un peu partout dans le mot de passe.

- Utilisez un mot de passe qui contient des caractères alphanumériques et qui inclus de la ponctuation (si cela est supporté par le système).

- Utilisez au moins 6 caractères, et au moins 8 si vous êtes sous Windows.

- Utilisez une sélection pseudo aléatoire de lettres et de nombres.

- Utilisez un mot de passe qui peut être saisie rapidement, sans avoir à regarder le clavier. Ceci rend plus difficile à une personne de voler votre mot de passe en regardant votre clavier (par dessus votre épaule).

- Changez de mot de passe régulièrement. Plus le compte est critique (comme le compte "root" sous Unix ou "Administrateur" sous Windows), plus il faut changer de mot de passe fréquemment. Une personne qui aurait réussi à avoir un accès serait alors stopper par ces changements et ne pourrait plus continuer à utiliser cet accès.

Le point commun de toutes ces règles réside dans le fait que le mot de passe doit être facile à mémoriser. On évitera les mots de passe qui doivent être écrit sur un bout de papier pour pouvoir être retrouvés. S'il n'est pas mémorisable, une personne tierce pourrait trouver ce morceau de papier et ainsi compromettre l'identité d'un utilisateur et donc sa sécurité. Le plus important dans une politique de mot de passe est de sensibilisé l'utilisateur final au maximum.

→ Server Policy

Pour correspondre au minimum de sécurité souhaitée, nous choisissons de ne pas implémenter de sécurité au niveau des serveurs mail, dns, dhcp, web.

→ **Router Policy**

Cisco 3620 :

Notre routeur de tête Cisco 3620, implémente les VLANs de niveau 2 et ne s'occupe pas de la sécurité. Le mot de passe d'accès à la console du routeur suit la police de sécurité des mots de passe définit plus haut.

Routeurs Parc et Métier :

Sysctl est une interface qui permet d'effectuer un paramétrage d'un système Linux en fonctionnement. Cela comprend de nombreuses options avancées de la pile protocolaire TCP/IP et du système de mémoire virtuelle qui sont à double tranchant mais peuvent améliorer les performances pour un administrateur système expérimenté. Pour cette phase, nous utiliserons les options de base, celle qui permet de router et celle qui change le Time To Live.

L'utilisation de NetFilter/IPtables est freinée, car nous nous situons dans la phase 1. Il n'a été implémenté que les fonctions les plus courantes trouvées dans les politiques de sécurité.

Politique par défaut des IPTables :

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

Ne prend pas en compte les paquets fragmentés :

```
iptables -A INPUT -f -j DROP
```

Fonctions implémentées au niveau des IPTables :

- Requête interne sur interface de loopback autorisé
- Suivi de communication TCP, UDP, ICMP
- Routage de services vers les machines concernées
- Demandes de connexions TCP et UDP acceptées
- Définition d'une poubelle propre où nous enlevons du réseau les paquets invalides

La lecture séquentielle des règles fera que les paquets non autorisés seront mis à la poubelle.

3.3.2 Description de la phase 2

Appliquons maintenant un niveau de sécurité qui correspond mieux à ce qui se trouve dans le milieu professionnel. Pour des besoins de tests comparatifs de sécurité, nous ne changerons pas la sécurité sur les postes clients.

Comme la sécurité doit être évolutive, il existe plusieurs façons de faire évoluer notre architecture :

- de manière basique, c'est-à-dire la solution 1,

- de façon poussée, c'est-à-dire la solution 2.

Nous n'implémentons que la solution la plus basique et expliquons la solution plus poussée.

3.3.2.1 Solution 1 de sécurité basique

Pare-feu :

Pour bien configurer son pare-feu, il suffit de bien respecter les conseils suivants :

- Essayez de limiter l'accès à votre réseau à des utilisateurs connus utilisant une adresse IP statique. Vous pourrez ainsi rejeter toutes les autres requêtes venant d'utilisateurs utilisant une adresse IP non autorisée. Vous effectuez de la sorte un filtrage au niveau IP.
- Fermez tous les ports en écoute sur les différents serveurs et ouvrez seulement ceux dont vous avez besoin. Filtrez ces ports, c'est-à-dire rejetez toutes les autres requêtes sur les autres ports que ceux en écoute.
- Empêchez toutes les connexions sortantes sur des services non autorisés. Pour cela, il suffit de définir un nombre limité de services auxquels les serveurs et les clients peuvent accéder (mail, ftp, web...). Ensuite, il faut configurer le pare-feu pour rejeter les connexions depuis l'intérieur vers l'extérieur sur des services différent de ceux définis.

La politique de sécurité de nos routeurs est telle qu'elle accepte tout ce qui est OUTPUT. La première constatation est qu'il est difficile de parler de sécurité si l'on ne considère pas les chaînes OUTPUT.

La première étape lors d'une attaque est de déterminer les règles de firewalling. Le but est simple : savoir quels ports ne sont pas filtrés avec le scan et le firewalking.

Routeur Cisco :

Sera supprimé sur ce routeur les services inutiles, la gestion des protocoles non utilisés et la prise en main du routeur par d'autre voix que la console.
En configurant, l'IOS des routeurs Cisco, nous avons implémenté le *flowcontrol*, des timers bien contrôlés qui permettront de fermés des sessions ouverts inactives, de limiter le nombre de sessions simultanées, la modification des bannières, la définition des utilisateurs avec leurs mot de passe chiffrés, la redéfinition des privilèges pour ces utilisateurs et bien sûr des *Access List* (ACL).

Routeurs :

Pour les routeurs qui se retrouvent dans des positions critiques de notre architecture, nous implémenterons un niveau de sécurité du noyau adapté avec le patch de la GrSecurity2 et une configuration de noyau beaucoup

plus fine. Pour la communication entre nos sous-réseaux, nous utiliserons un outil pour les chiffrer. Les moyens utilisés pour réaliser cela dépendront de la facilité et la rapidité d'implémentation. Sachant que le but n'est de mettre en place le meilleur chiffrage de données résistant à toute attaque, nous avons choisit, pour sa facilité de déploiement : OpenVPN. Le routeur de tête du parc informatique sera donc logiquement relié à l'autre routeur, créant ainsi une nouvelle architecture.

Serveur WEB :

Le serveur Web basé sur l'architecture LAMP (Linux, Apache, MySQL, PHP) hébergerait un site Internet répondant à des critères de sécurité plus poussés.

Serveur Mail :

Les mails utilisent un serveur SMTP qui sert à envoyer des mails sur le réseau local ou sur Internet. Ce service est en écoute sur le port 25.

- Le premier problème avec un serveur SMTP est qu'il peut servir de relais de mailing anonyme. Un pirate peut très bien s'en servir pour envoyer des mails scabreux à travers Internet.
- Un autre problème concerne les commandes EXPN et VRFY : ces commandes sont des sources de nombreuses informations pour le pirate. Il convient de les désactiver si le logiciel de messagerie le permet.

→ Comment s'en protéger ? : Appliquez des règles de firewalling assez strictes concernant le serveur SMTP (usage réservé exclusivement aux machines du réseau interne) et choisir un MTA en conséquence.

Serveur DNS :

Le serveur DNS se retrouvera sur un seul de nos routeurs et sera configuré correctement et de manière sécurisé. Un serveur DNS est en écoute sur le port 53. Les attaques suivantes concernent les faiblesses du protocole DNS (Le DNS ID Spoofing, le DNS Cache Poisoning).

Proxy WEB :

Les clients qu'on ne touche pas spécialement sont sujets à problèmes. Pour cela, sans pour autant changer leur configuration, on peut remédier à ce problème de sécurité. La mise en place d'un mandataire WEB est une des solutions. Pour cela, on placera sur le routeur du parc informatique, le trio SQUID/SQUIGUARD/CHASTITY-LIST et une configuration adaptée.

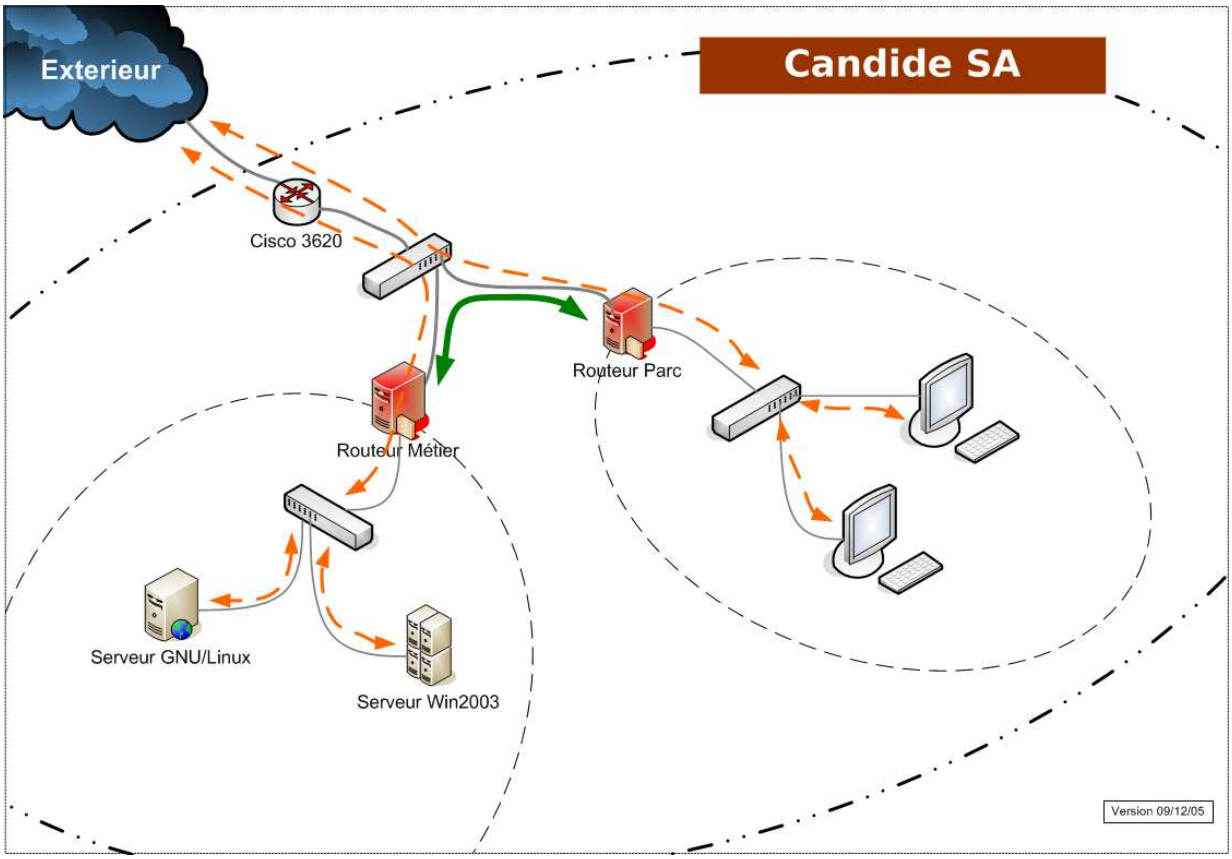
Serveur DHCP :

Malheureusement, le protocole DHCP comporte diverses failles :

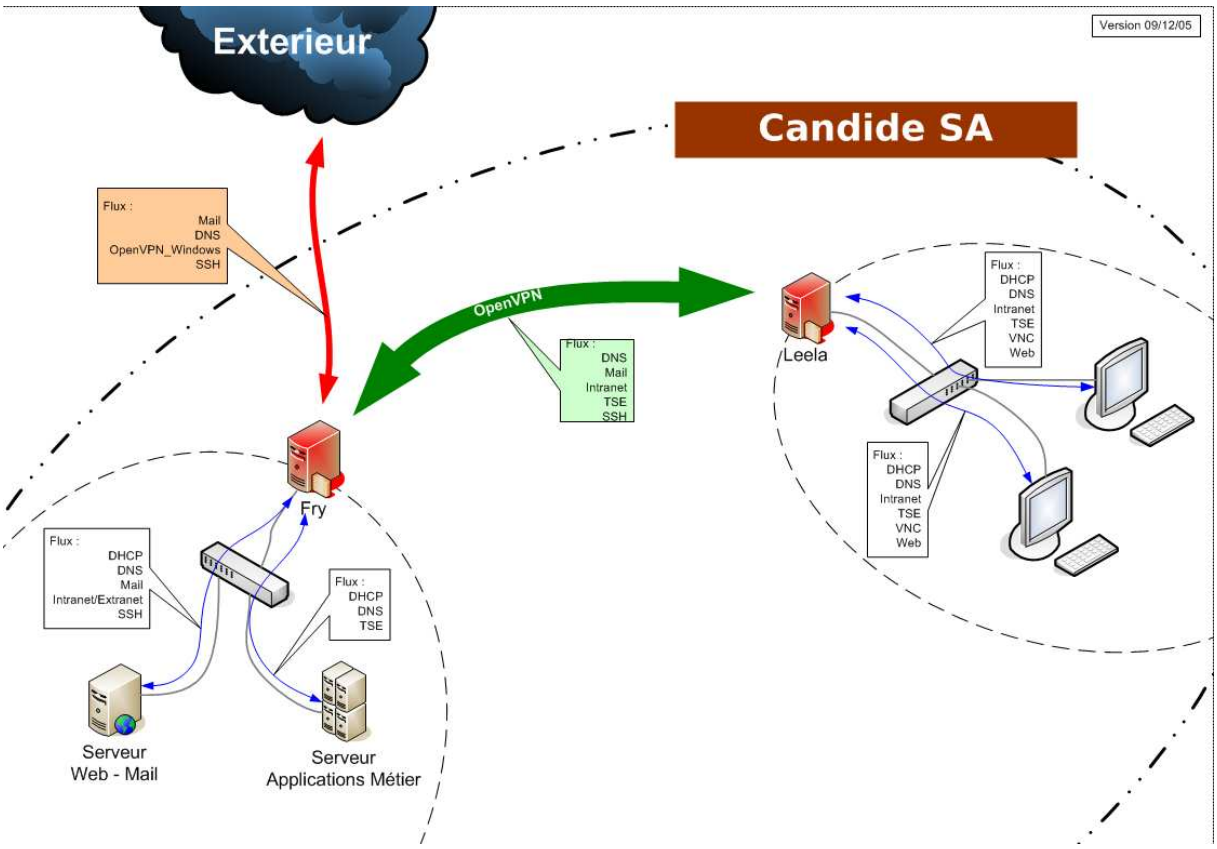
- Faux serveurs DHCP,
- Attaque par épuisement des ressources.

Ce service sera supprimé dans la phase 2.

Pour résumer, nous obtenons le schéma suivant :



Et donc un schéma plus précis qui correspond à :



3.3.2.2 Solution 2 de sécurité poussée

Cette solution ne sera pas implémentée totalement car le temps nous manque.

Elle consiste en :

- changer les routeurs en véritables passerelles de niveau 2. Celles-ci n'auraient plus d'adresse IP et ne seront plus visible au niveau Réseaux du modèle OSI. Elles garderont leur efficacité de filtrage, mais les règles seront adaptées à ce type d'architecture. Pour les serveurs, les règles et configurations seront les mêmes.
- Changer les empreintes de pile TCP/IP grâce à l'outil Morph pour permettre, lors de scans réseau, de masquer les systèmes d'exploitation que nous utilisons.
- Appliquer une politique de sécurité pour les postes clients, spécifiée par la NSA. Et seront installés sur ces postes, un pare-feu et un antivirus complets et mises à jour.
- Mettre en place d'un système de leurre à l'aide de l'outil HoneyNet.
- Changer le routeur Cisco 3620 par un Cisco 2611 qui dispose d'un noyau *IP Advanced Services*
- Marquer les paquets de la Candide SA pour simplifier les règles de filtrage.

3.3.2.3 Politiques mises en place

→ Acceptable Use Policy

Les utilisateurs possèdent un compte Windows, un compte mail, et un compte web. Pour chacun de ces services, un mot de passe sera confié aux utilisateurs et sera inchangeable. Il n'est pas autorisé aux utilisateurs d'utiliser le web à des fins personnels.

Les logiciels Peer-To-Peer ne sont pas tolérés. L'installation de logiciels par les utilisateurs est interdite. Seuls les administrateurs systèmes sont habilités à installer un logiciel. Pour cela, les utilisateurs possèdent un compte Windows restreint en droit.

Ils sont responsables de leurs actes en intranet ou sur Internet.

Les machines clients seront mises à jour par les administrateurs qui installeront un pare-feu et un anti-virus.

→ Email Policy

Les utilisateurs peuvent consulter uniquement leur compte mail professionnel sur les serveurs de l'entreprise via les protocoles de l'entreprise.

Rappel : aucune installation de client de messagerie n'est autorisée. Seuls les administrateurs ont le pouvoir d'installer un client email sécurisé tel que Thunderbird, qu'ils mettront à jour à chaque fois que cela sera nécessaire.

Les virus et le spam sont directement supprimés par le serveur, mais sera quand même installé sur les machines, des logiciels de surveillance et de suppression de malware.

→ Password Policy

La politique de mot de passe complète celle définie dans la phase 1. Les mots de passe des administrateurs seront changés toutes les semaines**.**

La complexité du mot de passe sera pour cela testée par différents logiciels spécialisés dans le casse de mot de passe, tels que « John The Ripper » et ses compagnons.

→ Server Policy

Le service DNS devient sécurisé et nous définirons plusieurs vues du réseau, une vue d'extérieure et une vue d'intérieure pour limiter la découverte de notre plan d'adressage. De plus, le DNS est mis en place sur un seul des routeurs.

Le serveur mails s'occupe de l'archivage et assure l'authentification. Il est aussi capable de lutter contre le spam et les virus.

Les bannières et les messages d'aide ou de bienvenue d'un service réseau en écoute pouvant donner des informations sur les versions de logiciel ou le système sont retirés.

Pour la communication entre les routeurs, nous ferons du tunneling qui a pour effet de créer virtuellement un réseau interne. De plus, ces communications seront chiffrées, offrant ainsi une sécurité accrue.

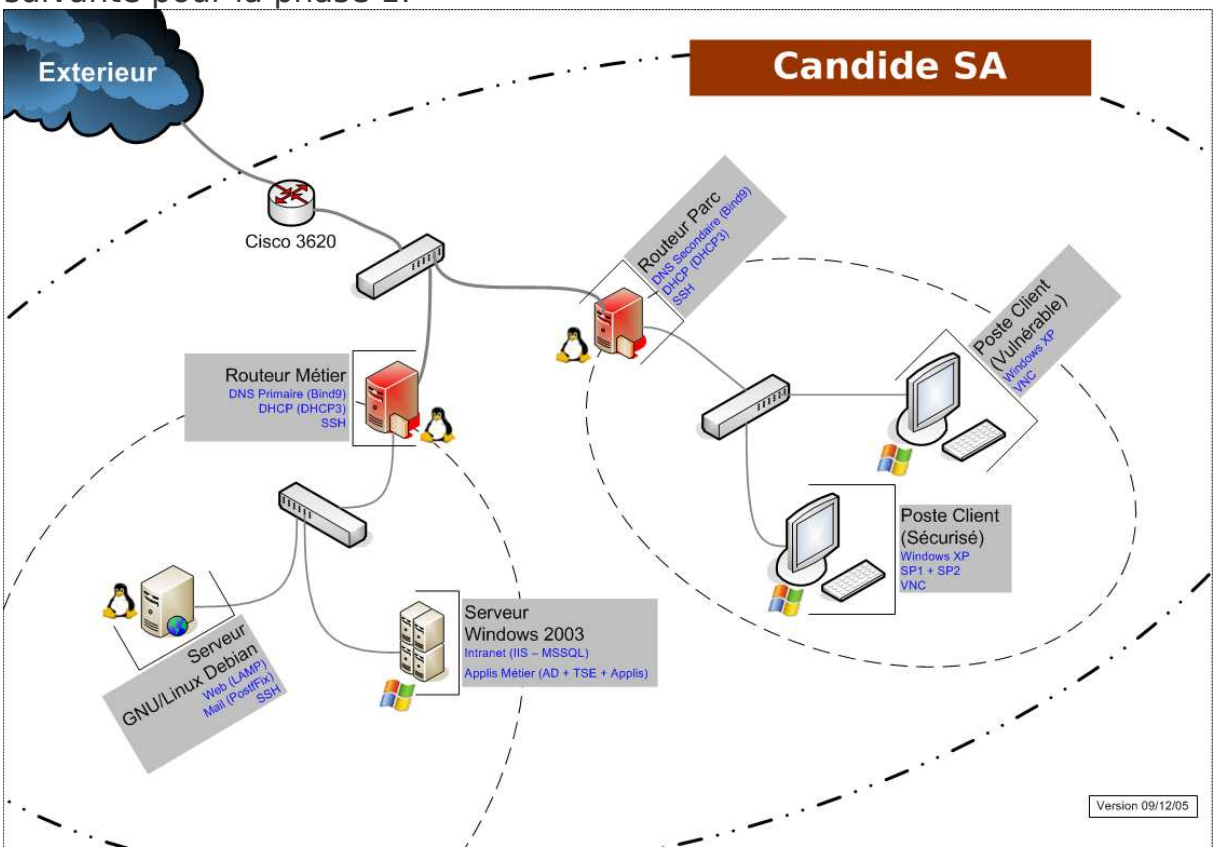
→ Router Policy

Pour améliorer la sécurité, nous supprimons la fonctionnalité VLAN et mettons en place la politique de sécurité conseillée par la NSA dans le document : *Router Security Configuration Guide*.

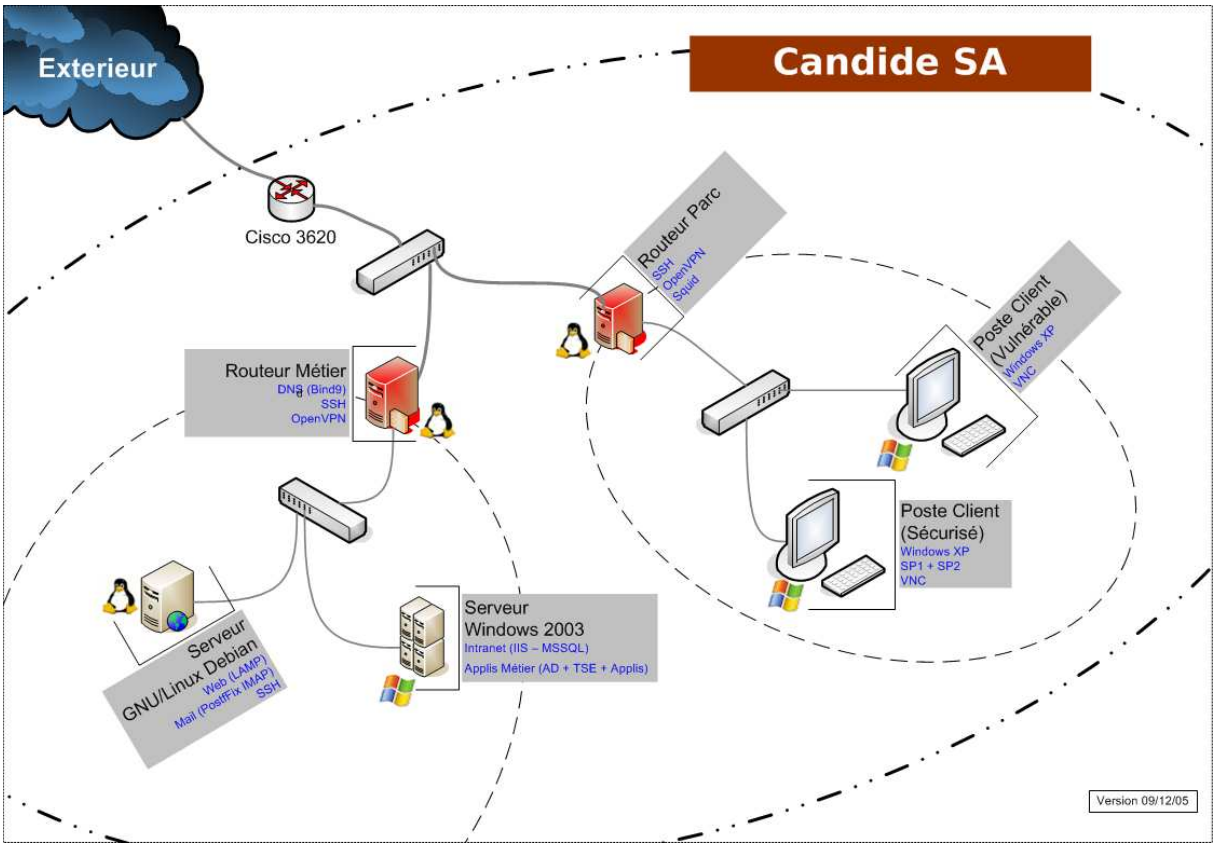
4 ETUDE DETAILLEE DU CAHIER DES CHARGES

4.1 Association Service – Matériel

Nous avons donc réparti les services sur les machines de la manière suivante pour la phase 1:



Et pour la phase 2 :



Nous disposons d'une configuration matérielle identique sur toutes les machines de CandideSA : AMD Athlon XP 2600+, 128 Mo de mémoire vive, et 8 Go de disque dur. Cette configuration est une configuration insuffisante de nos jours mais nous avons dû faire avec afin d'offrir le maximum de services qui sont en place dans les entreprises.

Les utilisateurs étant familiarisés avec un environnement Microsoft, les postes de travail sont des Windows XP.

Si pour les postes de travail cette configuration est tolérée, il n'en est rien pour des serveurs d'entreprise. Malgré cela et afin d'offrir aux employés de CandideSA les services métiers les plus courants, nous avons dû mettre en place un Windows 2003 Server sur la machine *Bender*.

Les produits Microsoft étant assez onéreux à l'achat, nous avons choisi des systèmes GNU/Linux Debian Sarge pour nos routeurs *Fry* et *Leela* ainsi que pour le serveur *Zoidberg*.

Le serveur Windows 2003 dispose des services IIS et MS-SQL Server pour les applications métier.

Le serveur Debian *Zoidberg* héberge les services Web et Mail. Pour le service Web, nous choisissons Apache et le module PHP3-MySQL qui permet la création d'une base de données pour le site Web. Pour le service Mail, indispensable dans une entreprise, nous choisissons Postfix.

Pour attribuer les adresses IP automatiquement aux clients, en phase 1, et permettre d'intégrer facilement des postes nomades, le service DHCP est obligatoire. Les routeurs sont dédiées au DHCP et au DNS qui assure la résolution de nom.

4.2 Etude de la sécurité

4.2.1 Mise en place effective de la phase 1

Pour correspondre au minimum de sécurité souhaitée, nous avons choisi de ne pas implémenter de sécurité au niveau des serveurs mail, dns, dhcp, web.

Au niveau du service de résolution de noms (DNS), nous décidons de le répartir sur les 2 routeurs :

- Fry est définit comme serveur DNS primaire.
- Leela est définit comme serveur DNS secondaire.

Les serveurs répondront à toutes les requêtes transmises, qu'elles proviennent du réseau local ou de l'Internet.

Voici la configuration détaillée pour chaque élément du réseau :

- Clients :

- Adresse IP : attribution automatique par le serveur DHCP
- Configuration DNS : adresse IP de Leela

- Serveur Zoidberg :

- Service web :
  - Installation d'**Apache** et de **php3-mysql**
  - Installation de **mysql-server**
  - Création d'un compte root de la base de données indépendant du compte root système
  - Création d'une base de données
  - Mise en place d'un site web utilisant **mysql**
- Service mail :
  - Installation du package **postfix 2.2 patchlevel 7** avec sa configuration par défaut
  - Installation du démon IMAP **courrier-imapd**
- Service SSH :
  - Ecoute sur le port 22
  - Seul l'utilisateur **admfirewall** peut se connecter
  - Pour être root, il faut s'identifier en tant que **admfirewall** puis **SU** (i.e. se logguer en root)

- Routeurs :

Au niveau des routeurs d'entrée de parc, nous avons décidé de mettre le minimum de sécurité.

Fonctions implémentées au niveau des IPTables :

- Requête interne sur interface de loopback autorisé,
- Suivi de communication TCP, UDP, ICMP,
- Définition d'une poubelle propre où nous enlèvons de notre réseau les paquets invalides,
- Nous laissons passer les demandes de connexions TCP, UDP,
- Routage de services vers les bonnes machines.

Configuration de Fry :

- Installation de Debian avec un noyau Linux 2-6-12
- Installation du pare-feu NetFilter
- Configuration nécessaire des Sysctl

  - Service DHCP
    - Installation du package **dhcp3-server**
    - Ecoute sur le port standard sur l'interface côté réseau interne
    - Dans la plage d'adresses IP 192.168.10.0/24
    - Adresses se terminant par 250, 251, 252 et 253 non attribuées en prévision de l'ajout d'équipements d'interconnection ou serveurs
    - Adresse IP se terminant par 254 attribuée à la passerelle
    - Les autres adresses sont distribuables par le serveur

  - Service DNS
    - Installation du package **bind9**
    - Serveur primaire de la zone **candide.com**
    - Déclaration des 6 machines du réseau.

  - Service SSH :
    - Ecoute sur le port 22
    - Seul l'utilisateur **admfirewall** peut se connecter
    - Pour être root, il faut s'identifier en tant que **admfirewall** puis **SU** (i.e. se logguer en root)

Configuration de Leela :

- Installation de Debian avec un noyau Linux 2-6-12
- Installation du pare-feu NetFilter
- Configuration nécessaire des Sysctl

- Service DHCP
  - Installation du package **dhcp3-server**
  - Ecoute sur le port standard sur l'interface côté réseau interne
  - Dans la plage d'adresses IP, attribution statique par adresse MAC pour les 2 serveurs
  - Adresses se terminant par 250, 251, 252 et 253 non attribuées en prévision de l'ajout d'équipements d'interconnection ou serveurs
  - Adresse IP se terminant par 254 attribuée à la passerelle
  - Les autres adresses sont distribuables par le serveur

- Service DNS
  - Installation du package bind9
  - Serveur secondaire qui se réfère à *Fry*.

- Service SSH :
  - Ecoute sur le port 22
  - Seul l'utilisateur **admfirewall** peut se connecter
  - Pour être root, il faut s'identifier en tant que **admfirewall** puis **SU** (i.e. se logguer en root)

4.2.2 Mise en place effective de la phase 2

Voici la configuration détaillée pour chaque élément du réseau :

- Clients :

- Installation du pare-feu **Kerio Personnal Firewall 4.2.2**
- Installation de l'antivirus **AVG 7.1**

- Routeurs :

- Pour la résolution de noms (DNS), nous décidons de concentrer uniquement le service sur le routeur Fry, avec la configuration de différentes vues à la manière de CYMRU.
- Pour la communication entre les 2 équipements, la solution choisie est de chiffrer leur communication à l'aide de OpenVPN, ce qui aura pour effet de créer virtuellement un réseau interne.
- Fry et Leela sont modifiés en passerelles filtrantes.
- De plus, voici en détail les changements apportés :

  - Sur la passerelle Fry :
    - Suppression du serveur DHCP
    - Installation d'un serveur DNS sécurisé

- Mise en place d'un mot de passe sur le BIOS
- Mise en place d'un mot de passe LILO et suppression de l'option **FAILSAFE**
- Suppression des services de base inutiles (portmap, …)
- Suppression du prompt **Root** du noyau
- Interdiction du démarrage sur disquette
- Restriction des redémarrages systèmes depuis la console
- Installation **GRSecurity2**, un outil de sécurisation du noyau Linux
- Installation **ArpWatch**, un outil de sécurisation ARP
- Désactivation des programmes **finger** et **auth** (ou **ident**)
- Installation du module **rp_filter**, un outil de filtrage des paquets

➢ Sur la passerelle Leela :

- Suppression du serveur DHCP
- Suppression du serveur DNS
- Mise en place d'un mot de passe sur le BIOS
- Mise en place d'un mot de passe LILO et suppression de l'option **FAILSAFE**
- Suppression des services de base inutiles (portmap, …)
- Suppression du prompt **Root** du noyau
- Interdiction du démarrage sur disquette
- Restriction des redémarrages systèmes depuis la console
- Installation **GRSecurity2**, un outil de sécurisation du noyau Linux
- Installation **ArpWatch**, un outil de sécurisation ARP
- Désactivation des programmes **finger** et **auth** (ou **ident**)
- Installation du module **rp_filter**, un outil de filtrage des paquets
- Installation de Squid, SquidGuard et Chastity-List permettant de concentrer les requêtes http des utilisateurs et proposé un service sécurisé.

- Serveur Zoidberg :

- Le service mail s'occupe de l'archivage de mail et assure l'authentification grâce au MTA PostFix et ses modules de sécurité (TLS-auth)
- Il utilisera le protocole IMAP pour le MDA
- Installation de **SpamAssassin**, pour filtrer le spam
- Installation de **Clam** pour lutter contre les virus

- Installation de **Amavisd-new** pour faire la relation entre les différents outils ce qui présentent un avantage certain,
- Interdiction du relayage SMTP
- Suppression des bannières donnant les versions de logiciel et les messages d'aide ou de bienvenue d'un service réseau en écoute

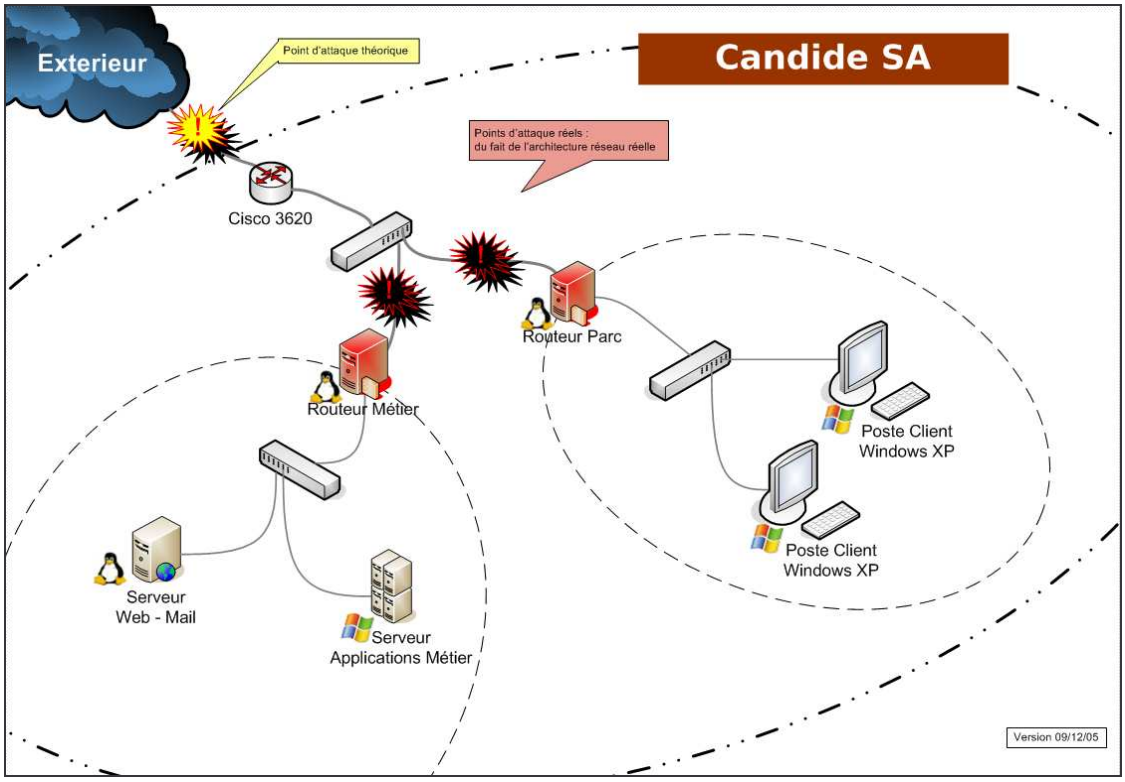
Les principales configurations des serveurs, routeurs se retrouverons en fichier, joint à ce rapport. Parmi ces configurations, vous retrouverez notament :

- les configurations IPTable,
- les configurations Sysctl,
- la configutation du routeur 3620.

5 RETOUR SUR INVESTISSEMENTS

5.1 Etude des risques

Après étude de notre architecture, nous avons identifié les points d'attaque possibles.
Le schéma ci-dessous les recense :



Comme nous pouvons le voir, les attaques peuvent réellement survenir au niveau des 2 routeurs d'entrée de chaque sous réseau.
En effet, il s'agit des points d'entrée sur le réseau de Candide SA et, hormis une attaque en interne par une personne malintentionnée qui aurait pénétrée dans les locaux de l'entreprise, il s'agit des points les plus sensibles généralement recensés sur les réseaux.

5.2 Communication

Nous nous sommes mis en relation avec l'équipe Analyse afin d'obtenir les informations concernant le trafic généré sur notre réseau.
En effet, les rapports de cette équipe doivent nous permettre de mettre en évidence les attaques subies.
Nous leur avons donc ouvert des ports afin qu'ils accèdent à notre réseau via un tunnel VPN. Pour des raisons indépendantes de notre volonté, nous n'avons pas obtenu de rapports d'analyse.

Toutefois, en cas d'attaque, nous avions au préalable défini les actions à entreprendre.

5.3 Gestion des incidents

Les attaques ont différents objectifs :

- exploit technologique
- vol d'informations
- altération des informations
- arrêt du service
- …

Pour ces raisons, les conséquences d'une attaque sont plus ou moins importantes. En effet, le vol d'information n'a pas de conséquence sur le fonctionnement du réseau, mais son importance est plus que relative car il peut s'agir d'espionnage industriel et donc de pertes de parts de marché à terme.

La plupart de nos services étant basés sur du logiciel libre, le coût de réparation ne se chiffre qu'en heures passées par l'ingénieur réseau de la société.

Concernant les systèmes à base de logiciel propriétaire, un contrat de maintenance pourra être conclu avec l'éditeur afin d'obtenir les correctifs de sécurité dès leurs sorties ou la réparation des dégâts causés par l'attaque par l'intervention d'un expert sur site.

Que faire donc en cas d'attaque ?

- isoler les machines infectées ou tout le parc contenant la machine
- débrancher le réseau de l'Internet
- mettre en place un service d'urgence
- réparer coûte que coûte
- attendre un audit de police
- …

La plupart des entreprises ont tendance à minimiser l'importance d'une attaque et à rétablir le fonctionnement du réseau le plus rapidement possible, sans au préalable en faire référence aux autorités judiciaires compétentes et sans effectuer d'audit interne de sécurité. Nous avons décidé, en cas de problème, de se concerter en premier lieu sur la gravité de l'attaque ainsi que sur la rentabilité et donc l'éventualité de réparer cette panne.

En appliquant la loi :

RISQUES = RENTABILITE x MENACES x COUTS

Nous pourrons être bien mesurer et auditer les risques. La politique à envisager est la continuité de service, c'est-à-dire la réparation des pannes précises, sans bavures et surtout sans débrancher le poste ou serveur concerné du réseau.

6 CONCLUSION

L'architecture du réseau est opérationnelle et le niveau de sécurité auquel nous sommes arrivés est très bon.

Le temps passé à configurer les machines sous GNU Linux a été sous-estimé et nous nous rendons compte que si Linux appartient au monde du logiciel libre et que sa licence est bon marché, il demande des connaissances qui se paient en heures de travail et cette solution a par conséquent un coût non négligeable compte tenu du niveau de technicité des ingénieurs nécessaires à son installation et à sa maintenance.

Ce projet nous a permis d'acquérir un grand nombre de connaissances car une veille technologique permanente est nécessaire afin de connaître les dernières techniques d'attaques ainsi que les dernières failles de sécurité découvertes pour chaque système d'exploitation.

Ce projet a été très intéressant et nous a demandé beaucoup d'investissement personnel. Il est intéressant dans le sens où il nous permet de se mettre dans les conditions de travail réelles en entreprise, ce qui est une bonne préparation avant notre intégration dans le milieu professionnel. La confiance entre collaborateurs est primordiale pour pouvoir avancer tous avec le même objectif et faire un travail efficace.

Nous avons eu quelques soucis au niveau les machines dédiées au projet avec des pannes matérielles qui peuvent être compensées par une redondance des équipements. Toutefois, ces pannes peuvent arriver et il était donc important que nous soyons confrontés à ce genre de problème.

Le point crucial dans tout travail d'équipe est la coordination et ce projet a mis en évidence la difficulté de communication à l'intérieur du groupe et avec les intervenants extérieurs, tel que le groupe Analyse.

Pour conclure, nous estimons avoir pris au sérieux ce projet et nous être investis du maximum qu'il nous était possible. Le résultat est concluant puisque aucune attaque n'a été recensée. Ce projet est une réussite d'équipe.

Projet Sécurité des SI

Annexes

Règles Routeur Cisco

----- Configuration générale

! -- Logging Conf
config t
! Configure logging timestamps and destinations.
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging buffered 4096 informational
! Journal !
! logging 192.168.5.5
! logging 192.168.5.55
clock timezone TIMEZONE 10
clock summer-time zone recurring
end

!Fait en plus
config t
line con 0
flowcontrol hardware in
flowcontrol software in
refuse-message #Ouned#
vacant-message #Attente longue !#
logout-warning 450
session-disconnect-warning 500
session-timeout 10
session-limit 2
absolute-timeout 10
end

! -- Time Out des connexions terminées non fermées
config t
line con 0
transport input none
login local
exec-timeout 5 0
exit

! -- Bannière
config t
banner motd # Equipement de la CandideSA #
banner login # Equipement de la CandideSA en attente de login #
banner prompt-timout # TimeOut #
end

! -- Utilisateur local
config t
username adminRouteur privilege 1 password #admin%routeur
username root privilege 15 password lemotdepasseadmin
end

! -- Port auxiliaire
config t
line aux 0
transport input none
login adminRouteur
exec-timeout 0 1
no exec
end

! -- VTY and remote Administration
config t
no access-list 90

```
access-list 90 deny any log
line vty 0 4
access-class 90 in
transport input none
login local
exec-timeout 0 1
no exec
end

! -- Privilege
!config t
!privilege exec level 15 connect
!privilege exec level 15 telnet
!privilege exec level 15 rlogin
!privilege exec level 15 show ip access-lists
!privilege exec level 15 show access-lists
!privilege exec level 15 show logging
!privilege exec level 1 show ip
!end

! -- Protection Mot de Passe
!config t
!enable secret XXX
!no enable password
!end

! -- Network Access
config t
ip telnet source-interface loopback0
access-list 99 permit 192.168.10.100 log
access-list 99 permit 192.168.10.101 log
access-list 99 deny any log
line vty 0 4
access-class 99 in
exec-timeout 5 0
transport input telnet
transport ouput none
login local
exec
end

! -- TCP keepalive
config t
service tcp-keepalives-in
end

! -- Accès via FTP
config t
ip ftp username AdminRouter
ip ftp password xxx
ip ftp source-interface loopback 0
end

! -- Télécharger fichier
!copy /erase ftp: startup-config ftp:


!----- IP and network services Section
config t
no cdp run
no ip source-route
no ip classless
no service tcp-small-serv
no service udp-small-serv
no ip finger
no service finger
```

```
no ip bootp server
no ip http auth local
no ip http server
no ip name-server
no ip domain-lookup
no autohangup
no exec-banner


! ----- Boot control section
no boot network
no service config

! ----- SNMP Section (for totally disabling SNMP)
! disable SNMP trap and system-shutdown features
no snmp-server enable traps
no snmp-server system-shutdown
no snmp-server trap-auth

! turn off SNMP alltogether
no snmp-server

! ----- Interface services section
interface eth 0/0
description Outside interface to 14.1.0.0/16 net
no ip proxy-arp
no ip directed-broadcast
no ip unreachable
no ip redirect
no ip mask-reply
ntp disable

interface loopback0
description Loopback interface for service bindings
no ip proxy-arp
no ip directed-broadcast
no ip unreachable
no ip redirect
no ip mask-reply
ntp disable

end

! ----- Access List

! -- Inbound traffic
config t
no access-list 100
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log
access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
access-list 100 deny ip host 255.255.255.255 any log
access-list 100 permit ip any 192.168.5.5 0.255.255.255
access-list 100 permit ip any 192.168.5.55 0.255.255.255
! -- Traceroute
access-list 100 deny udp any any range 33400 34400 log
! -- TCP/SYN Attack
access-list 100 permit tcp any 192.168.5.5 0.255.255.255 established
access-list 100 permit tcp any 192.168.5.55 0.255.255.255 established
access-list 100 deny tcp any range 0 65535 any range 0 65535 log
access-list 100 deny udp any range 0 65535 any range 0 65535 log
access-list 100 deny ip any any log
interface eth0/0
description "external interface"
```

!ip address x.x.x.x 255.255.255.0

ip access-group 100 in
end

! -- Limite l'accès externe avec TCP Intercept
config t
ip tcp intercept list 101
access-list 101 permit tcp any 192.168.5.5 0.255.255.255
access-list 101 permit tcp any 192.168.5.55 0.255.255.255
access-list 100 deny tcp any range 0 65535 any range 0 65535 log
access-list 100 deny udp any range 0 65535 any range 0 65535 log
access-list 101 deny ip any any log
interface eth0/0
description "external interface"

!ip address x.x.x.x 255.255.255.0

ip access-group 101 in
end

! -- outbound traffic
config t
no access-list 102
access-list 102 permit ip any 192.168.5.5 0.255.255.255
access-list 102 permit ip any 192.168.5.55 0.255.255.255
access-list 102 permit udp any any range 33400 34400 log
access-list 100 deny tcp any range 0 65535 any range 0 65535 log
access-list 100 deny udp any range 0 65535 any range 0 65535 log
access-list 102 deny ip any any log
interface eth0/0
description "internal interface"

!ip address x.x.x.x 255.255.255.0

ip access-group 102 in
end

! -- Land Attack
config t

!access-list 103 deny ip host x.x.x.x host x.x.x.x log

access-list 103 permit ip any any
interface eth0/0
description "external interface"

!ip address x.x.x.x 255.255.255.0

ip access-group 103 in
end

! -- Smurf Attack
config t

!access-list 104 deny ip any host x.x.x.x log
!access-list 104 deny ip any host x.x.x.x log
interface eth0/0
description "external interface"

!ip address x.x.x.x 255.255.255.0

ip access-group 104 in

```
end

! -- DOS Attack
config t
! the TRINOO DDoS systems
access-list 105 deny tcp any any eq 27665 log
access-list 105 deny udp any any eq 31335 log
access-list 105 deny udp any any eq 27444 log
! the Stacheldraht DDoS system
access-list 105 deny tcp any any eq 16660 log
access-list 105 deny tcp any any eq 65000 log
! the TrinityV3 system
access-list 105 deny tcp any any eq 33270 log
access-list 105 deny tcp any any eq 39168 log
! the Subseven DDoS system and some variants
access-list 105 deny tcp any any range 6711 6712 log
access-list 105 deny tcp any any eq 6776 log
access-list 105 deny tcp any any eq 6669 log
access-list 105 deny tcp any any eq 2222 log
access-list 105 deny tcp any any eq 7000 log

interface eth0/0
description "external interface"

!ip address x.x.x.x 255.255.255.0

ip access-group 105 in
exit

interface eth0/0
description "internal interface"

!ip address x.x.x.x 255.255.255.0

ip access-group 105 in
end


! -- renforcement de firewall

access-list 106 permit tcp any host 192.168.5.5 eq 80
access-list 106 permit tcp any host 192.168.5.5 eq 443

access-list 106 permit udp any host 192.168.5.5 eq 53
access-list 106 permit tcp any host 192.168.5.5 eq 53

access-list 106 permit tcp any host 192.168.5.5 eq 25

access-list 106 deny udp any any
access-list 106 deny tcp any any

interface eth0/0
description "external interface"

!ip address x.x.x.x 255.255.255.0

ip access-group 106 in
exit
```

Règles IPTables Phase 1 { Fry }

```
#####################################################
################## Table nat ########################
#####################################################

*nat
:PREROUTING ACCEPT [1359:169246]
:POSTROUTING ACCEPT [173:29946]
:OUTPUT ACCEPT [1121:76986]
# flush
-F

# NAT__WEB_ADMINISTRATION
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65051 -j DNAT --to-destination 192.168.10.100:80

# NAT__WEB_CANDIDE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.10.100:80

# NAT__MAIL_CANDIDE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 25 -j DNAT --to-destination 192.168.10.100:25

# NAT__IMAP_CANDIDE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 143 -j DNAT --to-destination 192.168.10.100:143

# NAT__OPENVPN
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65199 -j DNAT --to-destination 192.168.10.101:65199
-A PREROUTING -i eth0 -p udp -m udp --dport 65199 -j DNAT --to-destination 192.168.10.101:65199

# SSH__ANALYSE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65125 -j DNAT --to-destination 192.168.10.66:22

# NAT__MASQUERADING
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT


#####################################################
################ Table Filter #######################
#####################################################


*filter
:INPUT DROP [16:1280]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [59749:15842861]


#################### INPUT ##########################

# Suivi de communication
-A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT

# LOG des attaquants en INPUT
-A INPUT -s 192.168.5.2 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "ATTAQUANTS_INPUT: "
-A INPUT -s 192.168.5.2 -i eth0 -m limit --limit 10/sec -j DROP

# Confiance aux adresses Amis
-A INPUT -s 192.168.5.55 -m mac --mac-source AA:00:04:00:0A:04 -i eth0 -j ACCEPT
-A INPUT -s 192.168.5.1 -m mac --mac-source 00:10:5A:DE:9D:D7 -i eth0 -j ACCEPT
-A INPUT -s 172.16.240.1 -i eth0 -j ACCEPT
-A INPUT -s 192.168.5.0/255.255.255.0 -i eth0 -j ACCEPT

# BAD-ADDRESS sur l'interface externe
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-ADDRESS/rejected: "
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-ADDRESS/rejected: "
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -j DROP
```

```
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-ADDRESS/rejected: "
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-ADDRESS/rejected: "
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -j DROP
-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-ADDRESS/rejected: "
-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -j DROP
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-ADDRESS/rejected: "
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -j DROP

# loopBack
-A INPUT -i lo -d 127.0.0.1 -m state --state NEW -j ACCEPT

# Pas de fragements
-A INPUT -f -j DROP

# SSH + Secure Brute Force
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name SSH --rsource -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH --rsource
-j LOG --log-prefix "SSH_brute_force "
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH --rsource
-j DROP

# SSH du LAN
-A INPUT -i eth1 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT

# DHCP
-A INPUT -i eth1 -d 192.168.10.254 -p udp -m udp --dport 68 -m state --state NEW -j ACCEPT

# DNS
-A INPUT -i eth0 -s 192.168.5.55 -d 192.168.5.5 -m mac --mac-source AA:00:04:00:0A:04 -p udp -m limit --limit
5/sec -m udp --dport 53 -m state --state NEW -j ACCEPT
-A INPUT -i eth1 -s 192.168.10.0/255.255.255.0 -d 192.168.10.254 -p udp -m limit --limit 5/sec -m udp --dport 53
-m state --state NEW -j ACCEPT

# Pour NMap ?? ca marche po on dirait
-A INPUT -i eth0 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 1/sec -j ACCEPT

# Poubelle propre
-A INPUT -m state --state INVALID -m limit --limit 1/sec -j LOG --log-prefix "INVALID/rejected: "
-A INPUT -m state --state INVALID -j DROP
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable


################### FORWARD ######################
# Suivi de communications
-A FORWARD -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p icmp -m state --state ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
-A FORWARD -p udp -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags FIN,ACK,ACK RST -m limit --limit 1/sec -j ACCEPT

# Forward par defaut de l'interieur -> exterieur
#-A FORWARD -i eth1 -s 192.168.10.0/255.255.255.0 -o eth0 -m state --state NEW -j ACCEPT

-A FORWARD -i eth1 -o eth0 -m state --state NEW -j ACCEPT

# LOG des attaquants en INPUT
-A FORWARD -s 192.168.5.2 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "ATTAQUANTS_FORWARD: "
-A FORWARD -s 192.168.5.2 -i eth0 -m limit --limit 1/sec -j DROP

# WEB_SORTANT
#-A FORWARD -i eth1 -o eth0 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT

# WEB_ADMINISTRATION
-A FORWARD -i eth0 -d 192.168.10.100 -o eth1 -p tcp -m tcp --dport 65051 -m state --state NEW -j ACCEPT

# WEB_CANDIDE
-A FORWARD -i eth0 -d 192.168.10.100 -o eth1 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT

# MAIL
```

```
-A FORWARD -i eth0 -d 192.168.10.100 -o eth1 -p tcp -m tcp -m multiport --dports 25,143 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth1 -s 192.168.10.100 -o eth0 -j ACCEPT

# OPENVPN
-A FORWARD -i eth0 -d 192.168.10.101 -o eth1 -p tcp -m tcp --dport 65199 -m state --state NEW -j ACCEPT
-A FORWARD -i eth0 -d 192.168.10.101 -o eth1 -p udp -m udp --dport 65199 -m state --state NEW -j ACCEPT

# SSH__FORWARD_ANALYSE
-A FORWARD -i eth0 -d 192.168.10.66 -o eth1 -p udp -m udp --dport 22 -m state --state NEW -j ACCEPT

# Poubelle propre
-A FORWARD -m state --state INVALID -m limit --limit 1/sec -j LOG --log-prefix "INVALID/rejected: "
-A FORWARD -m state --state INVALID -j DROP
-A FORWARD -p icmp -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -j REJECT --reject-with tcp-reset
-A FORWARD -p udp -j REJECT --reject-with icmp-port-unreachable

# Clamp MSS TO MTU
-A FORWARD -o eth0 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
COMMIT
```

Règles IPTables Phase 2 { Fry }

```
####################################################
################## Table nat #######################
####################################################

*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
# flush
-F

################### PREROUTING #########################

# NAT__WEB_ADMINISTRATION
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65051 -j DNAT --to-destination 192.168.10.100:80

# NAT__WEB_CANDIDE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.10.100:80

# NAT__MAIL_CANDIDE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 25 -j DNAT --to-destination 192.168.10.100:25

# NAT__OPENVPN_WINDOWS
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65199 -j DNAT --to-destination 192.168.10.101:65199
-A PREROUTING -i eth0 -p udp -m udp --dport 65199 -j DNAT --to-destination 192.168.10.101:65199

# SSH__ANALYSE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65125 -j DNAT --to-destination 192.168.10.66:22
-A PREROUTING -i eth0 -p tcp -m tcp --dport 1241 -j DNAT --to-destination 192.168.10.66:1241


################### POSTROUTING ########################

# NAT__MASQUERADING
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT


####################################################
################ Table Filter ######################
####################################################

*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
# flush
-F

################### INPUT ########################

# Suivi de communication
-A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT

# LOG des attaquants en INPUT
```

```
-A INPUT -s 192.168.5.2 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "ATTAQUANTS_INPUT: "
#-A INPUT -s 192.168.5.2 -i eth0 -m limit --limit 10/sec -j DROP

# Confiance aux adresses Amis
-A INPUT -s 192.168.5.55 -m mac --mac-source AA:00:04:00:0A:04 -i eth0 -j ACCEPT
-A INPUT -s 192.168.5.1 -m mac --mac-source 00:10:5A:DE:9D:D7 -i eth0 -j ACCEPT
-A INPUT -s 172.16.240.1 -i eth0 -j ACCEPT
-A INPUT -s 192.168.5.0/255.255.255.0 -i eth0 -j ACCEPT

# BAD-ADDRESS sur l'interface externe
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -j DROP
-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -j DROP
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -j DROP

# loopBack
-A INPUT -i lo -d 127.0.0.1 -m state --state NEW -j ACCEPT

# Tunnel OpenVPN_LINUX Fry <-> Leela
-A INPUT -i tun0 -j ACCEPT

# OpenVPN_LINUX
-A INPUT -i eth0 -s 192.168.5.55 -d 192.168.5.5 -p udp -m udp --dport 18467 -m state --state NEW -j
ACCEPT

# SSH + Secure Brute Force
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name SSH --rsource -
j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name
SSH --rsource -j LOG --log-prefix "SSH_brute_force "
#-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name
SSH --rsource -j DROP

# SSH du LAN
-A INPUT -i eth1 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT

# DNS
#-A INPUT -i tun0 -s 192.168.5.55 -d 192.168.5.5 -p udp -m limit --limit 5/sec -m udp --dport 53 -m
state --state NEW -j ACCEPT
#-A INPUT -i tun0 -s 192.168.5.5 -d 192.168.5.55 -p udp -m limit --limit 5/sec -m udp --dport 53 -m
state --state NEW -j ACCEPT
#-A INPUT -i eth1 -d 192.168.10.254 -p udp -m limit --limit 5/sec -m udp --dport 53 -m state --state
NEW -j ACCEPT
#Sans limite pour l'instant
-A INPUT -i tun0 -s 192.168.5.55 -d 192.168.5.5    -p udp -m udp --dport 53 -m state --state NEW -j
ACCEPT
-A INPUT -i tun0 -s 192.168.5.5  -d 192.168.5.55   -p udp -m udp --dport 53 -m state --state NEW -j
ACCEPT
-A INPUT -i eth1                -d 192.168.10.254 -p udp -m udp --dport 53 -m state --state NEW -j
ACCEPT

# Pour NMap
```

```
-A INPUT -i eth0 -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 1/sec -j ACCEPT

# Poubelle propre
-A INPUT -m state --state INVALID -m limit --limit 1/sec -j LOG --log-prefix "INVALID/rejected: "
-A INPUT -m state --state INVALID -j DROP
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
# Pas de fragements
-A INPUT -f -j DROP


################### FORWARD ######################

# Suivi de communications
-A FORWARD -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p icmp -m state --state ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
#-A FORWARD -p udp -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j ACCEPT
#-A FORWARD -p tcp -m tcp --tcp-flags FIN,ACK,ACK RST -m limit --limit 1/sec -j ACCEPT

# Forward par defaut de l'interieur -> exterieur
-A FORWARD -i eth1 -o eth0 -m state --state NEW -j ACCEPT

# Tunnel OpenVPN_LINUX -> INTERNET
-A FORWARD -i tun0 -o eth0 -j ACCEPT

# Tunnel OpenVPN_LINUX -> LAN_METIER
-A FORWARD -i tun0 -d 192.168.10.0/255.255.255.0 -o eth1 -j ACCEPT

# LOG des attaquants en INPUT
-A FORWARD -s 192.168.5.2 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix
"ATTAQUANTS_FORWARD: "
-A FORWARD -s 192.168.5.2 -i eth0 -m limit --limit 1/sec -j DROP

# WEB_CANDIDE
-A FORWARD -i eth0 -o eth1 -d 192.168.10.100 -p tcp -m tcp --dport 80 -m state --state NEW -j
ACCEPT
-A FORWARD -i tun0 -o eth1 -d 192.168.10.100 -p tcp -m tcp --dport 80 -m state --state NEW -j
ACCEPT

# WEB_SORTANT
-A FORWARD -i eth1 -o eth0 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT
-A FORWARD -i tun0 -o eth0 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT

# WEB_ADMINISTRATION
-A FORWARD -i eth0 -o eth1 -d 192.168.10.100 -p tcp -m tcp --dport 65051 -m state --state NEW -j
ACCEPT

# MAIL
-A FORWARD -i tun0 -d 192.168.10.100 -o eth1 -p tcp -m tcp -m multiport --dports 25,143 -j ACCEPT
-A FORWARD -i eth1 -s 192.168.10.100 -o tun0 -j ACCEPT
-A FORWARD -i eth0 -d 192.168.10.100 -o eth1 -p tcp -m tcp --dport 25 -m state --state NEW -j
ACCEPT

# OPENVPN_WINDOWS
-A FORWARD -i eth0 -d 192.168.10.101 -o eth1 -p tcp -m tcp --dport 65199 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth0 -d 192.168.10.101 -o eth1 -p udp -m udp --dport 65199 -m state --state NEW -j
ACCEPT

# SSH__FORWARD_ANALYSE
```

```
-A FORWARD -i eth0 -d 192.168.10.66 -o tun0 -p tcp -m tcp --dport 22 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth0 -d 192.168.10.66 -o tun0 -p tcp -m tcp --dport 1241 -m state --state NEW -j
ACCEPT

# Poubelle propre
-A FORWARD -m state --state INVALID -m limit --limit 1/sec -j LOG --log-prefix "INVALID/rejected: "
-A FORWARD -m state --state INVALID -j DROP
-A FORWARD -p icmp -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -j REJECT --reject-with tcp-reset
-A FORWARD -p udp -j REJECT --reject-with icmp-port-unreachable

# Clamp MSS TO MTU
-A FORWARD -o eth0 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu

################### OUTPUT ######################

# Connexion sur lo
-A OUTPUT -o lo -j ACCEPT

# Suivi de communications
-A OUTPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A OUTPUT -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A OUTPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
-A OUTPUT -p udp -m limit --limit 10/sec -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j ACCEPT

# Tunnel OpenVPN_LINUX Fry <-> Leela
-A OUTPUT -o tun0 -j ACCEPT

# OpenVPN_LINUX
-A OUTPUT -o eth0 -d 192.168.5.55 -p udp -m udp --dport 18467 -m state --state NEW -j ACCEPT

# Analyste Nessus
-A OUTPUT -o eth0 -d 192.168.5.54 -p tcp -m tcp --dport 1241 -m state --state NEW -j ACCEPT
-A OUTPUT -o eth0 -d 192.168.5.54 -p tcp -m tcp --sport 1241 -m state --state NEW -j ACCEPT

# Autorisation SSH
-A OUTPUT -o tun0 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o eth0 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o eth1 -p tcp -m tcp --dport 22 -j ACCEPT

# WEB_CANDIDE
-A OUTPUT -o eth0 -p tcp -m tcp --sport 80 -j ACCEPT
-A OUTPUT -o eth1 -d 192.168.10.100 -p tcp -m tcp --dport 80 -j ACCEPT

# Autorisation DNS
-A OUTPUT -o tun0 -d 10.10.10.254 -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -o tun0 -s 10.10.10.254 -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -o eth0 -d 195.220.59.2 -p udp -m udp --dport 53 -j ACCEPT
#-A OUTPUT -o eth0 -p udp -m udp --dport 53 -j ACCEPT

# MAIL
-A OUTPUT -o eth0 -s 192.168.10.100 -p tcp -m tcp --sport 25 -j ACCEPT
-A OUTPUT -o tun0 -s 192.168.10.100 -p tcp -m tcp -m multiport --dports 25,143 -j ACCEPT
-A OUTPUT -o eth1 -d 192.168.10.100 -p tcp -m tcp -m multiport --dports 25,143 -j ACCEPT

# Poubelle propre
-A OUTPUT -m state --state INVALID -m limit --limit 1/sec -j LOG --log-prefix "INVALID/rejected: "
-A OUTPUT -m state --state INVALID -j DROP

COMMIT
```

Règles IPTables Phase 1 { Leela }

```
####################################################
################## Table nat #######################
####################################################

*nat
:PREROUTING ACCEPT [302:38727]
:POSTROUTING ACCEPT [8187:316109]
:OUTPUT ACCEPT [9875:384307]

# NAT__OPENVPN_HERMES_UDP
-A PREROUTING -i eth0 -p udp -m udp --dport 65198 -j DNAT --to-destination 192.168.20.50:65198

# NAT__OPENVPN_HERMES_TCP
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65198 -j DNAT --to-destination 192.168.20.50:65198

# NAT__OPENVPN_KIF_UDP
-A PREROUTING -i eth0 -p udp -m udp --dport 65197 -j DNAT --to-destination 192.168.20.51:65197

# NAT__OPENVPN_KIF_TCP
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65197 -j DNAT --to-destination 192.168.20.51:65197

# NAT__SSH_MACHINE_ANALYSE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65125 -j DNAT --to-destination 192.168.5.5:65125

# NAT__OPENVPN_MACHINE_ANALYSE
-A PREROUTING -i eth0 -p udp -m udp --dport 65126 -j DNAT --to-destination 192.168.20.66

-A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128

# NAT__MASQUERADING
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT


####################################################
################ Table Filter ######################
####################################################


*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [19008:822082]


#################### INPUT ##########################

# Log des attaquants en INPUT
-A INPUT -s 192.168.5.2 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "ATTAQUANTS_INPUT: "

# Confiance aux adresses Amis
-A INPUT -s 192.168.5.5 -i eth0 -j ACCEPT
-A INPUT -s 192.168.5.1 -i eth0 -j ACCEPT
-A INPUT -s 172.16.240.1 -i eth0 -j ACCEPT
-A INPUT -s 192.168.5.0/255.255.255.0 -i eth0 -j ACCEPT
-A INPUT -s 192.168.10.0/255.255.255.0 -i eth0 -j ACCEPT
-A INPUT -s 192.168.20.0/255.255.255.0 -i eth0 -j ACCEPT
```

```
# BAD-ADDRESS sur l'interface externe
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -j DROP
-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -j DROP
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -j DROP

# loopBack
-A INPUT -d 127.0.0.1 -i lo -m state --state NEW -j ACCEPT

# Pas de fragements
-A INPUT -f -j DROP

# Suivi de communication
-A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT

-A INPUT -i eth1 -p tcp -m tcp --dport 3128 -j ACCEPT

# DHCP
-A INPUT -d 192.168.20.254 -i eth1 -p udp -m udp --dport 68 -m state --state NEW -j ACCEPT

# SSH + Secure Brute Force
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name SSH --rsource -
j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name
SSH --rsource -j LOG --log-prefix "SSH_brute_force "
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name
SSH --rsource -j DROP

# SSH du LAN
-A INPUT -i eth0 -s 192.168.5.5 -d 192.168.5.55 -p udp -m limit --limit 5/sec -m udp --dport 53 -m
state --state NEW -j ACCEPT

# DNS
-A INPUT -i eth0 -s 192.168.5.5 -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -i eth1 -s 192.168.20.0/255.255.255.0 -d 192.168.20.254 -p udp -m limit --limit 5/sec -m
udp --dport 53 -m state --state NEW -j ACCEPT
-A INPUT -i eth1 -s 192.168.20.0/255.255.255.0 -p udp -m limit --limit 5/sec -m udp --dport 53 -m
state --state NEW -j ACCEPT

# Pour NMap
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 1/sec -j ACCEPT

# Poubelle propre
-A INPUT -m state --state INVALID -m limit --limit 10/sec -j LOG --log-prefix "INVALID/rejected: "
-A INPUT -m state --state INVALID -j DROP
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
```

```
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable


################### FORWARD ######################

# LOG des attaquants en forward
-A FORWARD -s 192.168.5.2 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix
"ATTAQUANTS_FORWARD: "

# WEB SORTANT
-A FORWARD -i eth1 -o eth0 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT

# Mail SORTANT
-A FORWARD -i eth1 -o eth0 -p tcp -m tcp -m multiport --dports 25,143 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth1 -o eth0 -d 192.168.5.5 -p udp -m limit --limit 5/sec -m udp --dport 53 -m state --
state NEW -j ACCEPT

# Forward par defaut
-A FORWARD -i eth1 -o eth0 -p tcp --dport 80 -m state --state NEW -j ACCEPT

# OPENVPN
-A FORWARD -i eth0 -d 192.168.20.50 -o eth1 -p tcp -m tcp --dport 65198 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth0 -d 192.168.20.51 -o eth1 -p udp -m udp --dport 65197 -m state --state NEW -j
ACCEPT

# OPENVPN__ANALYSE
-A FORWARD -i eth0 -d 192.168.20.66 -o eth1 -p udp -m udp --dport 65126 -m state --state NEW -j
ACCEPT

# SSH__FORWARD_ANALYSE
-A FORWARD -i eth0 -d 192.168.5.5 -o eth0 -p tcp -m tcp --dport 65125 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth1 -o eth0 -s 192.168.20.66 -j ACCEPT
-A FORWARD -i eth0 -o eth1 -s 192.168.5.54 -j ACCEPT

#-A FORWARD -i eth0 -o eth1 -j ACCEPT
#-A FORWARD -i eth1 -o eth0 -j ACCEPT

# Suivi de communications
-A FORWARD -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p icmp -m state --state ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
-A FORWARD -p udp -m limit --limit 10/sec -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 10/sec -j ACCEPT

# Poubelle propre
-A FORWARD -m state --state INVALID -m limit --limit 10/sec -j LOG --log-prefix "INVALID/rejected: "
-A FORWARD -m state --state INVALID -j DROP
-A FORWARD -p icmp -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -j REJECT --reject-with tcp-reset
-A FORWARD -p udp -j REJECT --reject-with icmp-port-unreachable

# Clamp MSS TO MTU
-A FORWARD -o eth0 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
COMMIT
```

Règles IPTables Phase 2 { Leela }

```
#################################################
################## Table nat ####################
#################################################

*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-F
# NAT__OPENVPN_HERMES_UDP
-A PREROUTING -i eth0 -p udp -m udp --dport 65198 -j DNAT --to-destination 192.168.20.50:65198

# NAT__OPENVPN_HERMES_TCP
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65198 -j DNAT --to-destination 192.168.20.50:65198

# NAT__OPENVPN_KIF_UDP
-A PREROUTING -i eth0 -p udp -m udp --dport 65197 -j DNAT --to-destination 192.168.20.51:65197

# NAT__OPENVPN_KIF_TCP
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65197 -j DNAT --to-destination 192.168.20.51:65197

# NAT__SSH_MACHINE_ANALYSE
-A PREROUTING -i eth0 -p tcp -m tcp --dport 65125 -j DNAT --to-destination 192.168.5.5:65125

# NAT__OPENVPN_MACHINE_ANALYSE
-A PREROUTING -i eth0 -p udp -m udp --dport 65126 -j DNAT --to-destination 192.168.20.66

# NAT__MASQUERADING
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT


#################################################
################ Table Filter ###################
#################################################


*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-F

#################################################
######## TUN
###

-A INPUT -i tun0 -j ACCEPT
-A OUTPUT -o tun0 -j ACCEPT


-A INPUT -i eth0 -s 192.168.5.5 -d 192.168.5.55 -p udp -m udp --dport 18467 -m state --state NEW -j
ACCEPT
-A OUTPUT -o eth0 -d 192.168.5.5 -p udp -m udp --dport 18467 -m state --state NEW -j ACCEPT

#-A INPUT -i eth1 -s 192.168.5.55 -d 192.168.5.5 -p udp -m udp --dport 18467 -m state --state NEW
-j ACCEPT

################### INPUT ########################

# Log des attaquants en INPUT
```

```
#-A INPUT -s 192.168.5.2 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix "ATTAQUANTS_INPUT: "

# Confiance aux adresses Amis
-A INPUT -s 192.168.5.5 -i eth0 -j ACCEPT
-A INPUT -s 172.16.240.1 -i eth0 -j ACCEPT
-A INPUT -s 192.168.10.0/255.255.255.0 -i eth0 -j ACCEPT
-A INPUT -s 192.168.20.0/255.255.255.0 -i eth0 -j ACCEPT
#-A INPUT -s 192.168.5.1 -i eth0 -j ACCEPT
#-A INPUT -s 192.168.5.0/255.255.255.0 -i eth0 -j ACCEPT


# BAD-ADDRESS sur l'interface externe
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 0.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 127.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 10.0.0.0/255.0.0.0 -i eth0 -j DROP
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 172.16.0.0/255.240.0.0 -i eth0 -j DROP
#-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
#-A INPUT -s 192.168.0.0/255.255.0.0 -i eth0 -j DROP
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -m limit --limit 10/sec -j LOG --log-prefix "BAD-
ADDRESS/rejected: "
-A INPUT -s 224.0.0.0/224.0.0.0 -i eth0 -j DROP

# loopBack
#-A INPUT -d 127.0.0.1 -i lo -m state --state NEW -j ACCEPT
-A INPUT -i lo -m state --state NEW -j ACCEPT

# Pas de fragements
-A INPUT -f -j DROP

# Suivi de communication
-A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT

# PROXY
-A INPUT -i eth1 -s 192.168.20.0/24 -p tcp -m tcp --dport 3128 -m state --state NEW -j ACCEPT

# SSH + Secure Brute Force
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name SSH --rsource -
j ACCEPT
#-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name
SSH --rsource -j LOG --log-prefix "SSH_brute_force "
#-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl --name
SSH --rsource -j DROP

# Pour NMap
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 1/sec -j ACCEPT

# Poubelle propre
-A INPUT -m state --state INVALID -m limit --limit 10/sec -j LOG --log-prefix "INVALID/rejected: "
-A INPUT -m state --state INVALID -j DROP
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
```

```
################## FORWARD ######################

# LOG des attaquants en forward
-A FORWARD -s 192.168.5.2 -i eth0 -m limit --limit 1/sec -j LOG --log-prefix
"ATTAQUANTS_FORWARD: "

-A FORWARD -i eth1 -o tun0 -j ACCEPT
-A FORWARD -i tun0 -o eth1 -j ACCEPT

# Mail SORTANT
-A FORWARD -i eth1 -o tun0 -p tcp -m tcp -m multiport --dports 25,143 -m state --state NEW -j
ACCEPT

# DNS SORTANT
-A FORWARD -i eth1 -o tun0 -d 192.168.5.5 -p udp -m limit --limit 5/sec -m udp --dport 53 -m state --
state NEW -j ACCEPT
-A FORWARD -i eth0 -o tun0 -s 192.168.5.5 -p udp -m limit --limit 5/sec -m udp --dport 53 -m state --
state NEW -j ACCEPT

# OPENVPN
-A FORWARD -i eth0 -d 192.168.20.50 -o eth1 -p tcp -m tcp --dport 65198 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth0 -d 192.168.20.50 -o eth1 -p udp -m udp --dport 65198 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth0 -d 192.168.20.51 -o eth1 -p tcp -m tcp --dport 65197 -m state --state NEW -j
ACCEPT
-A FORWARD -i eth0 -d 192.168.20.51 -o eth1 -p udp -m udp --dport 65197 -m state --state NEW -j
ACCEPT

# OPENVPN__ANALYSE
-A FORWARD -i eth0 -d 192.168.20.66 -o eth1 -p udp -m udp --dport 65126 -m state --state NEW -j
ACCEPT

# SSH__FORWARD_ANALYSE
-A FORWARD -i eth0 -d 192.168.5.5 -o eth0 -p tcp -m tcp --dport 65125 -m state --state NEW -j
ACCEPT

# Suivi de communications
-A FORWARD -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A FORWARD -p icmp -m state --state ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
-A FORWARD -p udp -m limit --limit 10/sec -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 10/sec -j ACCEPT

# Poubelle propre
-A FORWARD -m state --state INVALID -m limit --limit 10/sec -j LOG --log-prefix "INVALID/rejected: "
-A FORWARD -m state --state INVALID -j DROP
-A FORWARD -p icmp -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -j REJECT --reject-with tcp-reset
-A FORWARD -p udp -j REJECT --reject-with icmp-port-unreachable

# Clamp MSS TO MTU
-A FORWARD -o eth0 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu

############################################################
##################
#############   Chaine Output
#####

# Suivi de communications
-A OUTPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A OUTPUT -p tcp -m state --state ESTABLISHED -m tcp ! --tcp-flags SYN,RST,ACK SYN -j ACCEPT
-A OUTPUT -p tcp -m state --state RELATED -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
-A OUTPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 3 -m state --state RELATED -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 11 -m state --state RELATED -j ACCEPT
-A OUTPUT -p udp -m limit --limit 10/sec -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j ACCEPT

# Autorisation SSH
-A OUTPUT -o tun0 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o eth0 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o eth0 -p tcp -m tcp --sport 22 -j ACCEPT

# Autorisation Web
-A OUTPUT -o tun0 -p tcp -m tcp --dport 80 -m state --state NEW -j ACCEPT

# Autorisation DNS
-A OUTPUT -o tun0 -d 192.168.5.5 -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -o tun0 -s 192.168.5.5 -p udp -m udp --dport 53 -j ACCEPT

# Proxy
-A OUTPUT -o eth1 -p tcp -m tcp --sport 3128 -j ACCEPT

COMMIT
```